- załącznik nr 1 –

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Zintegrowany system zarządzania infrastrukturą IT

Specyfikacja Techniczna Oprogramowania Zintegrowanego Systemu Zarządzania Infrastrukturą Informatyczną.

MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

✓ wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping

✓ wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)

✓ wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci

✓ wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.

✓ wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku.

✓ wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze.

✓ wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie.

✓ wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny.

✓ zablokowania mapy urządzeń przed przypadkową edycją.

✓ serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów.

✓ serwerów pocztowych: - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem), - program ma możliwość wykonywania operacji testowych, - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.

✓ monitorowania serwerów WWW i adresów URL.

✓ cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.

✓ obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.

✓ obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID.

✓ obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych.

✓ monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych – graficzna prezentacja panelu switcha, - ruchu generowanego przez podłączone do portów stacje robocze.

✓ serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie.

✓ wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu.

✓ wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP. Program umożliwia również definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

W ZAKRESIE INWENTARYZACJI program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.

2. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.

3. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.

4. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.

5. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.

6. Umożliwia odczytanie numeru seryjnego (klucze licencyjne).

7. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.

8. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.

9. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).

10. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

✓ przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,

✓ tworzenia powiązań między zasobami a urządzeniami,

✓ tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,

✓ wskazania osób uprawnionych do użycia zasobów,

✓ definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,

✓ określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,

✓ określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,

✓ definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,

✓ importu danych z zewnętrznego źródła (.CSV),

✓ przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,

✓ tworzenia powiązań między zasobami a dokumentami w relacji 1:N,

✓ oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,

✓ ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,

✓ generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,

✓ generowania protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,

✓ archiwizacji i porównywania audytów zasobów,

✓ tworzenia kodów kreskowych dla zasobów,

✓ drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,

✓ inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej na system Android,

✓ inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),

✓ definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja").

Dodatkowo dostępny jest Agent inwentaryzacji na system Android.

Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.

2. Informacje o aplikacjach używanych w organizacji.

3. Tworzenie własnych wzorców aplikacji.

4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.

5. Informacje o komputerach, na których aplikacja została wykryta.

6. Zarządzanie posiadanymi licencjami.

7. Wskazywanie osób odpowiedzialnych za licencję.

8. Wskazanie użytkowników licencji. 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.

10. Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.

12. Zarządzanie posiadanymi licencjami: raport zgodności licencji. 13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe posiadają możliwość filtrowania elementów per oddział.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

✓ Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),

✓ Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,

✓ Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,

✓ Informacji o edytowanych przez użytkownika dokumentach,

✓ Historii pracy (cykliczne zrzuty ekranowe),

✓ Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),

✓ Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),

✓ Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,

✓ Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail. Program ponadto posiada możliwość:

✓ blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

✓ blokowania ruchu na wskazanych portach TCP/IP,

✓ blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,

✓ wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,

✓ przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),

✓ definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

PROGRAM UMOŻLIWIA REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. Moduł ten zawiera również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości oraz automatycznym oczyszczaniem historii rozmów) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic).

Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

Moduł pomocy zdalnej umożliwia również:

✓ pobieranie listy użytkowników z Active Directory,

✓ zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,

✓ zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,

✓ zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,

✓ tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii),

✓ automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,

✓ procesowanie zgłoszeń użytkowników z wiadomości e-mail,

✓ tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,

✓ wykonywanie operacji na wielu zgłoszeniach równocześnie,

✓ dołączanie załączników do zgłoszeń,

✓ rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,

✓ szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,

✓ wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,

✓ zrzuty ekranowe (podgląd pulpitu),

✓ dystrybucję oprogramowania przez Agenty,

✓ dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),

✓ zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,

✓ możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,

✓ planowanie nieobecności pracowników helpdesk,

✓ obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,

✓ generowanie raportów obsługi helpdesk,

✓ zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),

✓ zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),

✓ wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików.

MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.

3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.

5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.

3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.

4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.

5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

2. Podłączenie/odłączenie urządzenia przenośnego.

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

WSPIERANIE ZARZĄDZANIA CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania.

1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.

2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.

3. Statystyki aktywności podwładnych widoczne dla przełożonego.

4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.

5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.

6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.

7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.

8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.

9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.

10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).

11. Wskaźnik czasu poświęconego na aktywność produktywną.

12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.

13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.

14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji.

Portal informacyjny w formie platformy WWW

Oprogramowanie AxencenVision posiada również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardówwidgety są rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być:

✓ Udostępniana w trybie „tylko do odczytu" z zabezpieczeniem tokenem.

✓ Wyświetlana w trybie jasnym lub nocnym.

Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.

Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania:

✓ Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,

✓ Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,

✓ Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW,

✓ Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń,

✓ Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem),

✓ Produktywność dla grupy, Statystyki czasu nieproduktywnego.

Ochrona przed usunięciem

Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

Funkcjonalność Agenta

Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

Program dostępny jest w języku polskim, angielskim, bułgarskim i litewskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.

Ilość licencji: 30 szt

2. Notebook z systemem operacyjnym – 5 szt.

Notebook 1 – 4 szt.

Procesor: Procesor klasy x64. Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark - High End CPU's **wynik min.: 6270 punktów na dzień ogłoszenia postępowania.** (3.0 GHz - 4.1 GHz, 2 rdzenie/ 4 wątki, 6 MB cache)
Pamięć RAM: 8 GB (1 x 8 GB, DDR4, SO-DIMM, 2666 MHz, non-ECC)
Maksymalna ilość pamięci: 16 GB
Liczba gniazd pamięci (ogółem / wolne): 2 / 1
Dysk: 256 GB (SSD, PCIe, NVMe, M.2)
Ekran: 15.6" FullHD (1920 x 1080, 60 Hz, 16:9, WVA, Anti-Glare)
Grafika: Intel® UHD (Zintegrowana, Pamięć współdzielona)
Karta sieci LAN: Realtek RTL8111H (Zintegrowana, 1 Gb/s)
Karta sieci WLAN: Wi-Fi 5 (802.11ac)
Bluetooth: Bluetooth 4.1
Czytnik kart pamięci: SD Card Reader
Czytnik linii papilarnych: Tak
Urządzenie wskazujące: TouchPad
Podświetlana klawiatura: Tak
Klawiatura numeryczna: Tak
Kamera internetowa: HD RGB (720p)
Dźwięk: Wbudowane głośniki, Mikrofon
System: Microsoft Windows 10/11 Pro (64 bit)
Bateria: Litowo-Polimerowa (41 Wh, 3 ogniwa)
Złącza: 1 x HDMI 1.4, 2 x USB-A 3.2 Gen 1, 1 x USB-A 2.0, 1 x RJ-45 (LAN), 1 x Gniazdo combo(Słuchawki/mikrofon)
Bezpieczeństwo: Slot na linkę zabezpieczenia, TPM 2.0
Akcesoria w zestawie: Zasilacz sieciowy
Gwarancja: 3 lata gwarancji producenta (Next Business Day)

Notebook 2 – 1 szt.

Ekran	13.5" 2256 x 1504px
Matryca błyszcząca	IPS
Ekran dotykowy	Tak
Model procesora	Procesor klasy x64. Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark - High End CPU's **wynik min.: 8380 punktów na dzień ogłoszenia postępowania.** (1.20GHz - 3.70GHz, 6MB cache)
Liczba wątków:	8
Pamięć RAM	8GB 3733 MHz
Dysk twardy	256GB SSD M.2 PCIe
Karta graficzna	
Zintegrowana	Intel Graphics
System operacyjny	Windows 10
Komunikacja	Wi-Fi 6 AX, Bluetooth 5.0
Złącza	1 x USB 3.1 Gen 1 1 x USB Type-C 1 x Audio Jack
Multimedia	Kamera internetowa, Wbudowane głośniki , 2 x Mikrofon
Klawiatura	Klawiatura podświetlana

Bateria	Lithium-Ion (Li-Ion) 45.8 Wh

3. Pakiet biurowy – 4 szt.

Typ produktu	Pakiet biurowy zawierający: Edytor tekstu, Arkusz kalkulacyjny, Program pocztowy
Zastosowanie	Biurowe
Architektura programu	64-Bit
Typ DRM	Platforma producenta jak systemu operacyjnego
Rodzaj licencji	Komercyjna
Liczba stanowisk	1
Okres licencji	Dożywotnia
Wersja językowa	Wszystkie języki Eurozone
Rodzaj wydania	Licencja z kluczem aktywacyjnym
Dodatkowe informacje	Kompatybilny z systemami Windows oraz Mac

4. Serwer NAS

Procesor	4-core, 1.7GHz
Wbudowana pamięć RAM	4 GB
Maks. wielkość pamięci	8 GB
Rodzaj pamięci	SODIMM DDR3
Liczba obsadzonych gniazd pamięci	1
Liczba wszystkich gniazd pamięci	1
Wbudowana pamięć flash	512 MB
Liczba zainstalowanych dysków tw.	4
Maks. liczba dysków	4
Typ dysku	HDD
Format szerokości	3,5'' (LFF)
Interfejs dysku	SATA II - 3 Gb/s, SATA III - 6 Gb/s
RAID	Tak
Pozostałe parametry dysku	JBOD, Single, RAID 0, 1, 5, 6, 10, 50, 60
Architektura sieci	Gigabit Ethernet
Interfejs sieciowy	1 x 10Gbit/s SFP+, 1 x 10/100/1000/2500 Mbit/s, 1 x 10/100/1000 Mbit/s
Gniazda we/wy	2 x RJ-45 LAN, 3 x USB 3.0, 1 x SFP
Liczba wentylatorów	1
Wentylator	12 cm
Obudowa	Tower
Zasilanie	Zasilacz 90W, 100-240 V
Pozostałe parametry	Maks. liczba jednoczesnych połączeń (CIFS): 400

Parametry dysków twardych

Technologia CMR	Tak
Format	3.5''
Pojemność dysku	8 TB
Pamięć podręczna	256
Prędkość obrotowa	7200 obr./min.
Interfejs	SATA III (6 Gb/s)
Nominalny czas pracy	2 000 000 godzin

Oprogramowanie do Backup'u – licencja na 30 stanowisk komputerowych

Backup i przywracanie danych

- Deduplikacja danych na źródle,
- Backup przyrostowy i różnicowy,
- Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
- Backup danych lokalnych – plikowy oraz poczty Outlook,
- Backup otwartych plików (VSS),
- Filtr plików oraz folderów,
- Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),
- Wyłączanie komputera po wykonaniu backupu,
- Przywracanie danych do wskazanej lokalizacji,
- Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,
- Wyszukiwanie plików w repozytorium użytkownika,

Ustawienia

- Automatyczne logowanie,
- Zapamiętywanie danych logowania,
- Automatyczne uruchamianie programu przy starcie systemu,
- Ustawianie priorytetu dla procesu backupu,
- Zmiana klucza szyfrującego,
- Ustawienia przepustowości/zajętości pasma,
- Konfiguracja wydajności procesu backupu,

Bezpieczeństwo

- Zastępowanie nazwy pliku GUID-em,
- Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,
- Kompresja danych,
- Transmisja po bezpiecznym protokole TLS,
- Deklaracja klucza szyfrującego dane użytkownika,
- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,
- Obliczanie sumy kontrolnej,
- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.

WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS, Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Licencja obowiązuje przez okres minimum 12 miesięcy. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji.

5. Zestaw komputerowy – 2 szt.

Obudowa	Mini Tower
Procesor	Procesor klasy x64. Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark - High End CPU's **wynik min.: 8800 punktów na dzień ogłoszenia postępowania.** 3.6 GHz - 4.3 GHz, 4 rdzenie/ 8 wątków, 6 MB cache, 65 W
Pamięć RAM	8 GB (1 x 8 GB, DDR4, UDIMM, 2666 MHz, non-ECC)
Maksymalna ilość pamięci	64 GB
Liczba gniazd pamięci (ogółem / wolne)	2 / 1
Chipset	Oparta na chipsecie rekomendowanym przez producenta procesora.
Dysk	256 GB (SSD, PCIe, NVMe, M.2)
Grafika	Zintegrowana, oparta na chipsecie rekomendowanym przez producenta procesora.

Karta sieci LAN	Zintegrowana, 1 Gb/s
Karta sieci WLAN (802.11ac)	Oparta na chipsecie rekomendowanym przez producenta procesora
Bluetooth	Bluetooth 4.2
Dźwięk	Karta dźwiękowa (Zintegrowana)
Napęd optyczny	DVD+/-RW
Czytnik kart pamięci	SD Card Reader
System Operacyjny	System operacyjny musi być fabrycznie zainstalowany lub preinstalowany przez producenta komputera lub dostawcę komputera. Microsoft Windows 11 Pro (64 bit)
Sloty PCIe / M.2	1 x PCIe x16, 2 x PCIe x1, 1 x M.2 22x80mm
Złącza - panel przedni	2 x USB-A 3.2 Gen 1, 2 x USB-A 2.0, 1 x Gniazdo, uniwersalne audio
Złącza - panel tylni	1 x HDMI 1.4, 1 x VGA, 2 x USB-A 3.2 Gen 1, 2 x USB-A 2.0, 1 x RJ-45 (LAN), 1 x Wyjście liniowe audio
Moc zasilacza	260 W
Bezpieczeństwo	Slot na linkę zabezpieczenia
Akcesoria w zestawie	Przewód zasilający, Klawiatura przewodowa (Czarna), Mysz przewodowa (Czarna)
Gwarancja	3 lata gwarancji producenta (Next Business Day)

Monitor

Rodzaj wyświetlacza:	Monitor LCD z podświetleniem LED / matryca aktywna TFT
Klasa energii:	Klasa E
Wielkość przekątnej:	24"
Wielkość celownika:	23.8"
Typ panela:	IPS
Współczynnik kształtu:	16:9
Rozdzielczość natywna:	Full HD (1080p) 1920 x 1080 przy 60 Hz
Rozstaw pikseli:	0.2745 mm
Pikseli na cal:	93
Jasność:	250 cd/m²
Współczynnik kontrastu:	1000:1
Obsługa kolorów:	16,7 miliony kolorów
Czas reakcji:	8 ms (szary-do-szarego, normalny), 5 ms (szary-do-szarego, szybki)
Poziomy kąt widzenia:	178
Pionowy kąt widzenia:	178
Powłoka ekranu:	Antyrefleksyjna
Technologia podświetlenia:	Podświetlenie LED
Charakterystyka:	Paleta kolorów 72% (CIE 1931), paleta kolorów 83% (CIE 1976), technologia FlickerFree, Dell ComfortView, technologia Low Blue Light
Wymiary (szer./głęb./wys.):	55.264 cm x 17.1 cm x 33.161 cm - z podstawką
Złącza	
Interfejsy:	DisplayPort 1.2 VGA
Mechaniczne	

Regulacja pozycji ekranu:	Odchylenie
Kąt pochylenia:	-5/+21
Interfejs Montażowy VESA:	100 x 100 mm
Różne	
Cechy:	Slot blokady bezpieczeństwa (kabel blokady sprzedawany osobno), obsługuej interfejs VESA
Akcesoria w zestawie:	Osłona śruby VESA
Dołączone przewody:	1 x kabel DisplayPort 1 x kabel VGA
Zgodność z normami:	DisplayPort 1.2
Zasilanie	
Napięcie wejściowe:	AC 100-240 V (50/60 Hz)
Pobór Mocy SDR (tryb Wł.):	16 kWh/1000 godz.
Pobór Mocy (Standardowy):	16 wat
Pobór Mocy (Maksymalny):	28 wat
Zużycie energii w stanie czuwania:	0.3 wat
Zużycie energii w stanie uśpienia:	0.3 wat
Pobór mocy (tryb wył.):	0.3 wat
Standardy ochrony środowiska	
Certyfikat TCO:	TCO Certified Displays 8
EPEAT Compliant:	EPEAT Gold
Certyfikat ENERGY STAR:	Tak
Gwarancja producenta	
	36 miesięcy w miejscu instalacji

6. Urządzenie wielofunkcyjne

Cechy ogólne

Prędkość drukowania	20/25 str./min. (A4) 10/12 str./min. (A3)
Czas nagrzewania	Około 13 sekund (z trybu niskiego uśpienia)
Format i gramatura papieru	Kasety: A5R - A3, 60 - 163 g/m2 Pod. ręczny: 100 x 148 mm - A3, 60 - 209 g/m2
Pojemność papieru	1x 250 arkuszy (kaseta), 1x 100 arkuszy (podajnik ręczny) Maksymalnie 2900 arkuszy
Wewnętrzna taca odbioru	Pojemność 550 arkuszy
Automatyczny dupleks	A5R - A3, 60 - 163 g/m2
Panel użytkownika	Dotykowy, kolorowy panel LCD 26 cm (10.1”)
Pamięć	HDD 320 GB1), 2 GB RAM, Maks.: 4 GB RAM2)
Interfejsy	10Base-T/100Base-TX/1000Base-T, High Speed USB 2.0, WLAN2) (IEEE802.11b/g/n),

	Bluetooth2), Wi-Fi Direct2)

Drukowanie

Rozdzielczość	600 x 600 dpi, 5 bitów, 600 x 1200 dpi 1 bit tylko dla ster. PostScript
Języki opisu strony	PCL5e, PCL5c, PCL6 (PCL XL), XPS, PDF oraz emulacja PostScript 3
Wspierane systemy	Windows 10/8.1/7/Server 2008 (32/64 bity), Windows Server 2016/Server 2012 R2/Server 2012/Server 2008 R2 (64 bity), Mac OS X 10.6.8-10.13, Linux/Unix, Citrix, Novell SLES, SAP, AS/400
Protokoły sieciowe	TCP/IP (IPv4/IPv6), IPX/SPX, EtherTalk, NetBios po TCP/IP
Tryby koloru	Auto-Kolor (ACS), Kolor, Twin Kolor, B&W
Ustawienia koloru	Zarządzanie profilami ICC, Substytucja RGB, Jasność, Nasycenie, Kontrast, Balans Kolorów
Funkcje druku	Uniwersalny sterownik, Wtyczki (plug-ins2)) do sterownika, Wydruk z USB, Wydruk wstrzymany, Druk Tandemowy, Wydruk bezpośredni z E-mail

Skanowanie

Rozdzielczość	Maksymalnie 600 x 600 dpi
Prędkość skanowania	Podajnik RADF2): do 73 obr./min. (300 dpi) w kolorze i B&W
Tryby skanowania	Auto-Kolor (ACS), Kolor, Skala szarości, B&W
Formaty plików	JPEG/TIFF/XPS/PDF jedno i wielostronicowy, Zabezpieczony PDF, Slim PDF, PDF/A (A-1, A-2), Przeszukiwalny PDF2) (i inne edytowalne formaty jak DOCX, XLSX)2)
Funkcje skanowania	Skanowanie WS, do USB, do E-Mail, do pliku (SMB, FTP, FTPS, IPX/SPX, Lokalnie), z metadanymi (Meta Scan)2), do OCR2)3), do skrzynki (e-Filing), WIA, TWAIN

Kopiowanie

Rozdzielczość	Dla skanowania: 600 x 600 dpi Dla druku 600 x 600 dpi, równoważne 2400 x 600 dpi z wygładz. (tylko dla druku B&W)
Czas pierwszej kopii	Dla koloru: około. 9,5 sekundy Dla B&W: około 7,1 sekundy
	Zoom 25-400% (z szyby), 25-200% (z RADF)2)
Tryby kopiowania	Tekst, Tekst/Fotografia, Fotografia, Z wydruku, Mapa, Wygładzanie obrazu
Tryby koloru	Auto-Kolor (ACS), Kolor, Twin Kolor, Mono Kolor, Skala szarości
Ustawienia koloru	Odcień, Nasycenie, Balans Kolorów, Ustawienia koloru RGB,
Funkcje kopiowania	Elektroniczne sortowanie, Sortowanie z obrotem, Kopiowanie dokumentów, Usuwanie krawędzi, Tryby 2 - na - 1 / 4 - na – 1

7. Urządzenie UTM

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 5 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4.4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 800 Mbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 310 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy StatefulInspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - IntrusionPrevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Trafficshaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dlaprotokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.

- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja SafeSearch – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 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.

Wymagania ogólne

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. Dostawca wykona konfigurację urządzenia zgodnie z wytycznymi zamawiającego.
4. Wymagany co najmniej jeden inżynier posiadający certyfikat producenta na poziomie: NSE4, NSE5, NSE7.

8. System ochrony poczty

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony 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 platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, CitrixXenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

Funkcje serwera poczty

W tym zakresie dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.

4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.

Kontrola antyspamowa
System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty
System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania
W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.

4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)
System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu
W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie
System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Certyfikaty
Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje
System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu VirusOutbrake, Sandbox w chmurze, ochrona typu ClickProtect, Content Disarm&Reconstruction, Business Email Compromise na okres 12 miesięcy.

Gwarancja oraz wsparcie
1. System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Wymagania ogólne

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

3. Dostawca wykona konfigurację urządzenia zgodnie z wytycznymi zamawiającego.

4. Wymagany co najmniej jeden inżynier posiadający certyfikat producenta na poziomie: NSE4, NSE5, NSE7.

9. Oprogramowanie antywirusowe – Serwer

Wymagania dotyczące oprogramowania antywirusowego dla systemów typu Windows serwer:

1. Ochrona serwerów:
    a. Microsoft® Windows Server 2008 R2
    b. Microsoft® Small Business Server 2011, Standard edition
    c. Microsoft® Small Business Server 2011, Essentials
    d. Microsoft® Windows Server 2012
    e. Microsoft® Windows Server 2012 Essentials
    f. Microsoft® Windows Server 2012 R2
    g. Microsoft® Windows Server 2012 R2 Essentials
    h. Microsoft® Windows Server 2012 R2 Foundation
    i. Microsoft® Windows Server 2016 Standard
    j. Microsoft® Windows Server 2016 Essentials
    k. Microsoft® Windows Server 2016 Datacenter
    l. Microsoft® Windows Server 2016 Core
    m. Microsoft® Windows Server 2019 Standard
    n. Microsoft® Windows Server 2019 Essentials
    o. Microsoft® Windows Server 2019 Datacenter
    p. Microsoft® Windows Server 2019 Core
2. Ochrona całego systemu monitorowana i zarządzana z pojedynczej konsoli.
3. Zarządzanie aplikacją poprzez interfejs dostępny przez protokół https.
4. Możliwość określenia adresów sieciowych, z których można zarządzać aplikacją.
5. Możliwość określenia portu, na którym dostępny będzie interfejs zarządzający aplikacją.
6. Integracja z systemem anty wirusowym dla serwerów MS Exchange dostarczanym przez producenta poprzez wspólny lokalny interfejs zarządzający.
7. Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane.
8. Zintegrowany silnik „antyrootkitowy”.
9. Co najmniej dwa dedykowane silniki „antyspyware”.

10. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
11. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
12. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
13. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
14. Możliwość wywołania szybkiego skanowania pod kątem programów typu rootkit.
15. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.
16. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
17. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.
18. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
19. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „wirus", „keylogger", „dialer", „trojan".
20. Program powinien posiadać kwarantannę wirusów, spyware oraz riskware.
21. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.
22. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
23. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.
24. Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.
25. Automatyczne uruchamianie procedur naprawczych.
26. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
27. Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin.
28. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
29. Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona.
30. Możliwość zarządzania za pomocą centralnej konsoli

10. Oprogramowanie antywirusowe – Stacja robocza

Wymagania dotyczące system ochrony anty wirusowej z zaporą ogniową dla stacji roboczych.

1. Ochrona antywirusowa stacji roboczych:
   - Microsoft Windows 7 (32-bit i 64-bit)
   - Microsoft Windows 8.1 (32-bit i 64-bit)
   - Microsoft Windows 10 (32-bit i 64-bit)
2. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.
3. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.
4. Polski interfejs użytkownika aplikacji ochronnej.

Wymagania dotyczące technologii:

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.
2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.
3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".
4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
5. Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
6. Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
7. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
8. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
9. Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
10. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.
11. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
12. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
13. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".
14. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.
15. Ochrona pliku 'hosts' przed niepożądanymi wpisami.
16. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.
17. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.
18. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
19. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
20. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
21. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
22. Automatyczne uruchamianie procedur naprawczych.
23. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
24. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
25. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
26. Możliwość zablokowania wychodzącej wiadomości e-mail, jeżeli zostanie w niej wykryty zainfekowany załącznik.

27. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
28. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
29. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.
30. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.
31. Wsparciedlatechnologii Microsoft Network Access Protection (NAP).
32. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików.
33. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
34. Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako 'bankowość elektroniczna' poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.
35. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z daną witryną HTTPS.
36. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.
37. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.
38. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.
39. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
40. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
41. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)
42. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows
43. Moduł kontroli urządzeńzapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskietek).
44. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.
45. Moduł kontroli urządzeń umożliwia dodanie 'zaufanego urządzenia' poprzez podanie jego identyfikatora sprzętowego.

Wymagania dotyczące systemu zarządzania centralnego:

1. System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows oraz Linux.
2. Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych:
   - Windows Server 2008 SP1 64-bit: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server
   - Windows Server 2008 R2: Standard, Enterprise, Web Server
   - Windows Server 2012: Essentials, Standard, Datacenter
   - Windows Server 2012 R2: Essentials, Standard, Datacenter
   - Windows Server 2016; Essentials, Standard or Datacenter editions
   - Windows Server 2019; Essentials, Standard or Datacenter editions

3. Instalacja sytemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych:
   - Red Hat Enterprise Linux 6,7,8 64-bit
   - CentOS 6,7,8 64-bit
   - SuSE Linux Enterprise Server 11,12,15 64-bit
   - SuSE Linux Enterprise Desktop 11,12,15 64-bit
   - openSUSE Leap 43,15 64-bit
   - Debian GNU Linux 8,9 64-bit
   - Ubuntu 14.04,16.04,18.04 64-bit
4. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną.
5. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję.
6. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem).
7. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi.
8. Pełne centralne zarządzanie dla środowisk Windows Server 2003 (32-bit oraz 64-bit), Windows Server 2008 (32-bit oraz 64-bit), Windows Server 2008 R2, Windows Server 2012, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Linux.
9. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.
10. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
11. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.
12. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).
13. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.
14. Możliwość importu struktury drzewa z Microsoft Active Directory.
15. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.
16. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.
17. Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji.
18. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta.
19. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania.
20. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.
21. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.
22. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.
23. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji.
24. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).

25. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.
26. Możliwość eksportu raportów z pracy systemu do pliku HTML.
27. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.
28. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie".
29. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.
30. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe.
31. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy).
32. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.
33. Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.
34. System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.
35. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.
36. Możliwość przekierowania alertów bezpośrednio do serwera Syslog.
37. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
38. System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.
39. Pełna kopia bazy danych systemu zarządzania centralnego może być wykonywana automatycznie zgodnie z harmonogramem określonym przez administratora.
40. Administrator ma możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana.

11. Szkolenia dla pracowników w zakresie obsługi zakupionego sprzętu i oprogramowania

W ramach umowy wykonawca będzie zobowiązany do przeszkolenia pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania.