**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA - CZĘŚĆ I**

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Urządzenie klasy UTM – 1 szt.**
 |
| 1 | **Architektura systemu ochrony**: system ochrony musi być zbudowany przy użyciu pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanych układów. Producent urządzeń musi udzielić odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). |
| 2 | **System operacyjny**: dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia. |
| 3 | **Parametry fizyczne systemu:** nie mniej niż 8 portów Ethernet 10/100/1000 Base-TX. |
| 4 | **Funkcjonalności podstawowe i uzupełniające:** system ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności:1. kontrolę dostępu – zaporę ogniową klasy Stateful Inspection, ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, NNTP),
2. poufność danych – IPSec VPN oraz SSL VPN,
3. ochronę przed atakami – Intrusion Prevention System [IPS/IDS],
4. kontrolę treści i kategoryzację odwiedzanych stron WWW – Web\URL Filter,
5. kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP),
6. kontrolę pasma oraz ruchu [QoS, Traffic shaping],
7. kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM, P2P, VoIP, Web-mail),
8. zapobieganie przed wyciekiem informacji poufnej - DLP (Data Leak Prevention).
 |
| 5 | **Zasada działania (tryby)**: urządzenie musi dawać możliwość ustawienia jednego z dwóch trybów pracy: jako router/NAT (3.warstwa ISO-OSI) i jako most /transparent bridge/. |
| 6 | **Polityka bezpieczeństwa (firewall)**: polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać: adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie, zarządzanie pasmem sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ). Urządzenie musi umożliwiać utworzenie nie mniej niż 5.000 polityk firewall’a. |
| 7 | **Wykrywanie ataków**: wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) oraz niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP:1. nie mniej niż 4000 sygnatur ataków,
2. możliwość dodawania własnych sygnatur ataków,
3. możliwość wykrywania anomalii protokołów i ruchu.
 |
| 8 | **Moduł antywirusowy:** antywirus musi mieć możliwość transferu częściowo przeskanowanego pliku do klienta w celu zapobiegnięcia przekroczenia dopuszczalnego czasu oczekiwania (timeout). Antywirus musi przeprowadzać sprawdzanie danych zarówno po bazie sygnatur wirusów, jak i heurystycznie. |
| 9 | **Moduł antyspamowy**: moduł antyspamowy musi pracować w obrębie protokołów SMTP, POP3 i IMAP. Klasyfikacja wiadomości musi bazować na wielu czynnikach, takich jak:1. sprawdzenie zdefiniowanych przez administratora adresów IP hostów, które brały udział w dostarczeniu wiadomości,
2. sprawdzenie zdefiniowanych przez administratora adresów pocztowych,
3. RBL, ORDBL,
4. sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych.
 |
| 10 | **Filtracja stron WWW:** moduł filtracji stron www musi umożliwiać blokowanie stron w oparciu o:1. białe i czarne listy URL,
2. zawarte w stronie słowa kluczowe,
3. dynamicznie definiowane przez producenta kategorie.
 |
| 11 | **Translacja adresów**: statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT. |
| 12 | **Wirtualizacja i routing dynamiczny**: możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 4 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Obsługiwane protokoły routingu dynamicznego – co najmniej RIPv2, OSPF, BGP-4 i PIM. |
| 13 | **Połączenia VPN**: tworzenie połączeń w topologii Site-to-Site oraz Client-to-Site. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN). Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth. |
| 14 | **Uwierzytelnianie użytkowników**: system zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą:1. haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia,
2. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
3. haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych.

Rozwiązanie musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych. |
| 15 | **Wydajność**: obsługa nie mniej niż 1.100.000 jednoczesnych połączeń i 25.000 nowych połączeń na sekundę. Przepływność nie mniejsza niż 1 Gbps dla ruchu nieszyfrowanego i 250 Mbps dla VPN (3DES). Obsługa nie mniej niż 200 jednoczesnych tuneli VPN. |
| 16 | **Funkcjonalność zapewniająca niezawodność**: monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive. |
| 17 | **Konfiguracja i zarządzanie:** możliwość konfiguracji poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą mieć możliwość uwierzytelniania za pomocą:1. haseł statycznych,
2. haseł dynamicznych (RADIUS, RSA SecureID).

System musi umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. |
| 18 | **Raportowanie**: system musi mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym:1. zbieranie logów z urządzeń bezpieczeństwa,
2. generowanie raportów,
3. skanowanie podatności stacji w sieci,
4. zdalną kwarantannę dla modułu antywirusowego.
 |
| 19 | **Serwis oraz aktualizacje**: wykonawca musi dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres co najmniej 12 miesięcy. Urządzenie musi być objęte serwisem gwarancyjnym producenta przez okres co najmniej 12 miesięcy. |
| 20 | **Certyfikaty**: producent urządzeń musi posiadać co najmniej następujące certyfikaty: ISO 9001, UTM NSS Approved, EAL4+, ICSA Labs dla funkcji: Firewall, IPSec, SSL, Network IPS, Antywirus. |
| 21 | **Inne wymagania**: oferowane urządzenie musi zapewniać pełną i bezproblemową współpracę z już wdrożonymi rozwiązaniami w lokalizacji centralnej i delegaturach W-MUW, opartymi o urządzenia firmy FORTIGATE - modele 240D i 60D, szczególnie w zakresie zarządzania, zestawiania i utrzymywania połączeń gateway-to-gateway VPN (IPSec i SSL) oraz raportowania (Forti Analyzer). |

|  |  |
| --- | --- |
| **L.p.**  | **Parametry wymagane** |
| 1. **Odnowienie na kolejny rok usługi rocznego wsparcia dla urządzenia FortiGate – FG60D UTM – 6 szt.**
 |
| **Odnowienie na kolejny rok usługi rocznego wsparcia technicznego i aktualizacji dla urządzeń FortiGate – FG60D UTM Bundle (8x5 FortiCare plus NGFW, AV, Web Filtering and Antispam Services).** Rozpoczęcie usługi musi być liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi. Numery urządzeń zmawiającego: FGT60D4613031995, FGT60D4Q16031895, FGT60D4614033672, FGT60D4614032304, FGT60D4614032472, FGT60D4614033416. |

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Odnowienie na kolejny rok usługi rocznego wsparcia dla klastra urządzeń (2 urządzenia) FortiGate-240D UTM – 1 kpl.**
 |
| **Odnowienie na kolejny rok usługi rocznego wsparcia technicznego i aktualizacji dla a klastra urządzeń (2 urządzenia) FortiGate-240D UTM Bundle (8x5 FortiCare plus NGFW, AV, Web Filtering and Antispam Services).** Odnowienie wsparcia musi obejmować 2 urządzenia. Rozpoczęcie usługi musi być liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi. Numery urządzeń zmawiającego: FG240D4613801286, FG240D4613801331. |

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Odnowienie na kolejny rok usługi rocznego wsparcia dla urządzenia FortiGate - FG60C UTM – 1 szt.**
 |
| **Odnowienie na kolejny rok usługi rocznego wsparcia technicznego i aktualizacji dla urządzeń FortiGate – FG60C UTM Bundle (8x5 FortiCare plus NGFW, AV, Web Filtering and Antispam Services).** Rozpoczęcie usługi musi być liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi. Numer urządzenia zmawiającego: FGT60C3G11028367 |

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Odnowienie na kolejny rok usługi rocznego wsparcia dla urządzenia FortiGate – FG30D UTM – 1 szt.**
 |
| **Odnowienie na kolejny rok usługi rocznego wsparcia technicznego i aktualizacji dla urządzeń FortiGate – FG30D UTM Bundle (8x5 FortiCare plus NGFW, AV, Web Filtering and Antispam Services).** Rozpoczęcie usługi musi być liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi. Numer urządzenia posiadany przez zmawiającego: FGT30D3X14007168 |

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Aktualizacja oprogramowania antywirusowego z migracją do wersji z ochroną serwerów plikowych – 560 szt.**
 |
| 1 | **Zakres zamówienia.**1. Przedmiot zamówienia obejmuje aktualizację oprogramowania antywirusowego (odnowienie licencji dla ochrony 560 stacji roboczych) i bazy danych sygnatur wirusów oprogramowania obecnie eksploatowanego (ESET Endpoint Antivirus) w sieci komputerowej wraz z konsolą do zarządzania dla kompleksowej ochrony systemów komputerowych oraz migracją do wersji z ochroną serwerów plikowych – 560 szt.w Warmińsko-Mazurskim Urzędzie Wojewódzkim w Olsztynie oraz w Delegaturach Urzędu w Elblągu i Ełku, z aktualizacją roczną Rozpoczęcie usługi musi być liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi (lub krótszą – w zależności od dnia zawarcia umowy i terminu jej wykonania, bądź dostarczenie oprogramowania równoważnego) lub dostarczenie oprogramowania równoważnego w ilości 560 szt. Rozpoczęcie usługi musi być liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi.
2. Zamawiający dopuszcza możliwość zastosowania przez wykonawców w ofertach rozwiązań kompleksowej ochrony systemów komputerowych opierających się na innym – równoważnym oprogramowaniu, po spełnieniu warunków opisanych w punkcie 3, określających równoważność oprogramowania w stosunku do wskazanego w specyfikacji istotnych warunków zamówienia.
 |
| 2 | **Równoważność oprogramowania antywirusowego** w stosunku do określonego w specyfikacji istotnych warunków zamówienia. Przez równoważność oprogramowania należy rozumieć spełnienie następujących wymagań:1. oferowane oprogramowanie spełnia wymagania określone w punkcie 3 zawierającym specyfikację wymagań funkcjonalnych,
2. wykonawca wdroży oprogramowanie równoważne w nieprzekraczalnym terminie 3 dni roboczych od zawarcia umowy, czynności wykonywane będą w godzinach pracy zamawiającego tj. od 7:30 do 15:30 od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy,
3. wykonawca przeszkoli personel techniczny (6 osób) w zakresie używania, zarządzania oraz administrowania programem,
4. wykonawca przygotuje i przekaże zamawiającemu wersję elektroniczną instrukcji obsługi interfejsu użytkownika oprogramowania zainstalowanego na komputerze,
5. wykonawca dokona pełnej deinstalacji istniejącego oprogramowania w liczbie 560 licencji w następujących lokalizacjach: Olsztyn (budynek główny i 3 siedziby na terenie Olsztyna), Elbląg, Ełk, Grzechotki, Bezledy, Gronowo, Gołdap, łącznie z usunięciem wpisów w rejestrach systemowych,
6. wykonawca dokona zainstalowania oprogramowania na komputerach w liczbie zgodnej z liczbą wymaganych licencji (560 szt.).
 |
| 3 | **Specyfikacja wymagań funkcjonalnych.**1. **Ogólne:**
2. pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/Windows 10/Windows Server/Android,
3. wsparcie dla 32- i 64-bitowej wersji systemu Windows,
4. wersja programu dla stacji roboczych Windows dostępna w języku polskim,
5. pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim,
6. skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje takie jak ICSA labs lub Check Mark.
7. **Ochrona antywirusowa i antyspyware:**
8. pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami,
9. program musi oferować funkcję samo ochrony,
10. wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.,
11. skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików,
12. możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu,
13. system ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania,
14. możliwość skanowania dysków sieciowych i dysków przenośnych,
15. skanowanie plików spakowanych i skompresowanych,
16. możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń),
17. możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach,
18. możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu,
19. brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu,
20. możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej,
21. skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail,
22. możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie,
23. możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail,
24. skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie,
25. możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej,
26. w przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e‑mail,
27. możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie,
28. program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS,
29. program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe,
30. możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej,
31. możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych),
32. możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy,
33. możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu,
34. możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych,
35. dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe,
36. możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta,
37. możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła,
38. możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło,
39. hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo,
40. program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji,
41. program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu,
42. po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów,
43. program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach,
44. automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu,
45. możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami,
46. program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji,
47. program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http,
48. program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania,
49. wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
50. **Administracja zdalna:**
51. serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008, 2012 oraz systemach Linux,
52. serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL lub MySQL,
53. serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika,
54. serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy,
55. centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux,
56. centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android,
57. centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci,
58. zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta,
59. administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego,
60. agent musi przekazywać informacje na temat stanu systemu operacyjnego do Serwer administracyjna zarządzającego,
61. instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny,
62. instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym,
63. serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający,
64. serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu,
65. serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką,
66. serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy,
67. serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej,
68. serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów,
69. grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.,
70. serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania,
71. serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta,
72. edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej,
73. serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku,
74. serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta,
75. serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów,
76. serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania,
77. serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW,
78. raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS,
79. serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie,
80. serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące,
81. serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela,
82. narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia,
83. administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).
 |