**Załącznik nr 3 do SIWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Wymagania ogólne**

W skład systemu bezpieczeństwa będącego przedmiotem zamówienia wchodzą następujące elementy: firewall klasy NGFW/UTM , centralny system logowania, system ochrony przed zaawansowanymi zagrożeniami typu Sandbox.

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 10 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

W ramach postępowania wymaganym jest dostarczenie rozwiązania do analizy i wykrywania zaawansowanych i nieznanych zagrożeń za pomocą technologii „sandboxingu”.

**Urządzenie firewall klasy UTM.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | ***Szczegółowy opis oferowanych parametrów***  ***(nie dopuszcza się używania zwrotów np. „jak wymagane” lub podobnych)*** |
| 1. | **Wsparcie dla IPv4 i IPv6** | System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |  |
| 2. | **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. W ramach postępowania system musi zostać dostarczony w postaci redundantnej. 3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 4. Monitoring stanu realizowanych połączeń VPN. 5. System musi umożliwiać agregację linków, statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |  |
| 3. | **Interfejsy, Dysk, Zasilanie** | 1. System realizujący funkcję Firewall musi dysponować minimum:  * 2 portami Gigabit Ethernet RJ-45. * 16 gniazdami SFP+ 10 Gbps.  1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk SSD o pojemności minimum 480 GB. 4. System musi być wyposażony w zasilanie 2xAC. |  |
| 4. | **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 50 mln jednoczesnych połączeń oraz 400 000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 80 G bps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 50 Gbps dla pakietów 64 B. 4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 40 Gbps. 5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 50 Gbps. 6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 43 Gbps. 7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 13 Gbps. 8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 19 Gbps. |  |
| 5. | **Funkcje Systemu Bezpieczeństwa:** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 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 - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 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. 12. Analiza ruchu szyfrowanego protokołem SSH.   Powyższe funkcjonalności nie mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: |  |
| 6. | **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) dla protokołu SIP.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |  |
| 7. | **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/Counter Mode(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.  1. 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. |  |
| 8. | **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.   2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |  |
| 9. | **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. |  |
| 10. | **Kontrola Antywirusowa** | 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. 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. |  |
| 11. | **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. 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. 6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| 12. | **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 2100 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. |  |
| 13. | **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 avoidance. 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. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |  |
| 14. | **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.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| 15. | **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. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |  |
| 16. | **Logowanie** | 1. System musi mieć możliwość logowania 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 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. |  |
| 17. | **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. * ICSA lub NSS Labs dla funkcji IPS. * ICSA dla funkcji IPSec VPN.   ICSA dla funkcji SSL VPN. |  |
| 18. | **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:   * Kontrolę Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy. |  |
| 19. | **Gwarancja oraz wsparcie** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 8x5. |  |

**Centralny system analizy logów i raportowania.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | ***Szczegółowy opis oferowanych parametrów***  ***(nie dopuszcza się używania zwrotów np. „jak wymagane” lub podobnych)*** |
| 1. | **Interfejsy, Dysk, Zasilanie:** | 1. System musi dysponować co najmniej:  * 2 portami Gigabit Ethernet RJ-45.  1. Rozwiązanie musi dysponować powierzchnią dyskową min. 24 TB. 2. Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 1, 5, 6, 10, 50, 60. |  |
| 2. | **Parametry wydajnościowe:** | 1. System musi być w stanie przyjmować minimum 600 GB logów na dzień. 2. System musi być w stanie przeanalizować minimum 18 000 logów na sekundę. 3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 400 systemów. |  |
| 3. | **Logowanie** | 1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:   a. Listę najczęściej wykrywanych ataków.  b. Listę najbardziej aktywnych użytkowników.  c. Listę najczęściej wykorzystywanych aplikacji.  d. Listę najczęściej odwiedzanych stron www.  e. Listę krajów, do których nawiązywane są połączenia.  f. Listę najczęściej wykorzystywanych polityk Firewall.  g. Informacje o realizowanych połączeniach IPSec.   1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z i do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |  |
| 4. | **Raportowanie** | W zakresie raportowania system musi zapewniać:   1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |  |
| 5. | **Korelacja logów** | W zakresie korelacji zdarzeń system musi zapewniać:   1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System musi korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:  * Malware. * Aplikacje sieciowe. * Email. * IPS. * Traffic. * Systemowe: utracone połączenie VPN, utracone połączenie sieciowe. |  |
| 6. | **Zarządzanie** | 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczyć dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.   a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.   1. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |  |
| 7. | **Gwarancja oraz wsparcie** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 8x5. |  |

**System zaawansowanej ochrony przed zagrożeniami klasy Sandbox.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** | ***Szczegółowy opis oferowanych parametrów***  ***(nie dopuszcza się używania zwrotów np. „jak wymagane” lub podobnych)*** |
| 1. | **Wymagania techniczne:** | 1. rozwiązanie musi być fizyczną maszyną, nie może być wirtualną maszyną hostowaną na wirtualizatorze 2. - rozwiązanie musi umożliwiać montaż w standardzie 19” RACK 3. - rozwiązanie musi posiadać min. 2 porty 1 Gb/s RJ45 4. - rozwiązanie musi posiadać min. 2 wewnętrzne, redundantne, wymienne zasilacze Hot Swappable 5. - rozwiązanie musi posiadać min. 2 dyski twarde HDD o łącznej pojemności min. 500 GB |  |
| 2. | **Wydajność:** | 1. rozwiązanie musi pozwalać na przeanalizowanie w maszynach wirtualnych min. 150 plików na godzinę, 2. rozwiązanie musi pozwalać na przeskanowanie antywirusowe min. 5000 plików na godzinę, 3. rozwiązanie musi być oparte o dedykowany, autorski system operacyjny – nie dopuszcza się rozwiązań, gdzie platformą systemową jest system operacyjny ogólnego zastosowania, a na nim instalowane jest oprogramowanie jako aplikacja, 4. rozwiązanie musi umożliwiać analizę próbek dla wykonywanych na obrazach/maszynach wirtualnych następujących systemów operacyjnych: Windows XP, Windows 7, Windows 8.1, Windows 10, 5. rozwiązanie musi umożliwiać „pełny sanboxing”, rozumiany jako wykonanie w maszynie wirtualnej następujących rodzajów próbek: adres URL, dokumenty Microsoft Office, pliki wykonywalne (w tym języki skryptowe JavaScript, Visual Basic, PowerShell, bat), pliki PDF (Adobe Acrobat), pliki SWF (Adobe Flash) -  znajdujących się w wiadomościach pocztowych; 6. rozwiązanie musi umożliwiać uruchomienie min. 6 jednoczesnych instancji (umożliwienie jednoczesnej analizy 6 różnych próbek w ramach „pełnego sandboxingu”) maszyn wirtualnych, z możliwością rozbudowy, 7. rozwiązanie musi zawierać licencje na następujące produkty firmy Microsoft: Windows 7 (możliwość uruchomienia min. 6 instancji jednocześnie), Windows 10 (możliwość uruchomienia min. 6 instancji jednocześnie), Microsoft Office (możliwość uruchomienia min. 2 instancji jednocześnie), 8. rozwiązanie musi wspierać możliwość tworzenia własnych reguł, 9. rozwiązanie musi umożliwiać wgrywanie własnych obrazów systemów operacyjnych. W przypadku, kiedy ta funkcjonalność jest realizowana przez producenta i dodatkowo płatna, należy dostarczyć pakiet/voucher na możliwość utworzenia 10 obrazów systemów stworzonych przez Zamawiającego, 10. rozwiązanie musi umożliwiać, we współpracy z systemem poczty elektronicznej, kolejkowanie/zatrzymanie wiadomości pocztowej na czas analizy, tak aby wiadomość zawierająca złośliwy załącznik lub URL nie mogła trafić do użytkownika poczty przed uzyskaniem werdyktu, 11. rozwiązanie musi udostępniać API umożliwiające integracje z innymi systemami, 12. rozwiązanie musi umożliwiać rozbudowę integracji z następującymi klasami rozwiązań: zapora sieciowa nowej generacji (NGFW), systemy ochrony końcówek (Endpoint Protection Systems), 13. rozwiązanie musi umożliwiać cykliczne generowanie raportów, 14. rozwiązanie musi umożliwiać generowanie alertów podczas wykrywania zagrożeń i raportowanie ich za pomocą: Syslog, SNMP, SMTP, 15. rozwiązanie musi umożliwiać zarządzanie min. przez panel WebUI za pomocą przeglądarki internetowej, 16. rozwiązanie musi umożliwiać utworzenie klastra HA Active/Active z min. 4 urządzeń. Jeżeli funkcja klastrowania urządzeń traktuje jedno z nich jako primary i korzysta z jego zasobów, aby rozdzielać operacje na pozostałe urządzenia należy dostarczyć dodatkowo jedną maszynę wraz ze wszystkimi wymaganymi licencjami (fizyczną bądź wirtualną) do obsługi tej funkcjonalności, 17. sklastrowane urządzenia muszą pozwalać na zarządzanie z jednego miejsca (portalu, lub konsoli, lub aplikacji itp.). |  |
| 3. | **Gwarancja oraz wsparcie** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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 8x5. |  |
| 4. | **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:   * AV, IPS, Web Filtering, File Query, aktualizacje silnika Sandbox na okres 36 miesięcy, * Rozszerzenie licencji dla ochrony w oparciu o wersje systemów Windows 8 i 10. |  |

.....................................................................

*(upełnomocniony(ieni) przedstawiciel(e) Wykonawcy)*