# **Odnowienie usługi serwisowej dla klastra urządzeń Fortigate 600C**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L.p.** | **Nazwa urządzenia** | **Numer seryjny** | **Data rozpoczęcia serwisu [dzień-miesiąc-rok]** | **Typ serwisu** | **Miejsce instalacji** |
| **1** | **Fortigate 600C** | FG600C3914802391 | 2019-12-17 |  | Prokuratura Krajowa  ul. Rakowiecka 26/30  Warszawa |
| **Fortigate 600C** | FG600C3914800873 |
| **2** | **Inne wymagania** | 1. Wykonawca zapewni serwis gwarancyjny realizowany przez producenta rozwiązania lub Autoryzowanego Dystrybutora producenta. 2. Wykonawca zapewni dostęp wskazanego personelu Zamawiającego do dedykowanego portalu www producenta urządzenia, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do bazy wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp.. 3. Wykonawca zapewni możliwość zgłaszania na stronach www producenta sprzętu problemów eksploatacyjnych związanych z obsługą sprzętu będącego przedmiotem zamówienia. 4. Pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (nie tylko do serwisu Wykonawcy) przez cały okres świadczenia usług serwisowych. 5. Wykonawca w oferowanych pakietach serwisowych producenta zapewni dostęp do pomocy technicznej producenta (drogą telefoniczną, poprzez email lub stronę WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego. 6. **W ramach realizacji umowy Wykonawca dokona wymiany obecnie eksploatowanego klastra urządzeń Fortigate 600C na klaster urządzeń Fortigate 600E posiadający wszystkie licencje i subskrypcje jak dotychczas wykorzystywane rozwiązanie oraz zapewni dostęp do najnowszego oprogramowania i sygnatur do urządzenia objętego serwisem. Wykonawca będzie świadczył usługi serwisu gwarancyjnego dla tak dostarczonych urządzeń na warunkach określonych w umowie. Wykonawca dokona migracji konfiguracji z obecnie eksploatowanego rozwiązania do docelowego.** | | | | |
| **3** | **Warsztaty** | 1. Wykonawca dostarczy po 3 sztuki voucherów szkoleniowych na każdy poniższy kurs oraz 3 sztuki voucherów na autoryzowany egzamin NSE 4 (Network Security Professional):    1. NSE4 - FortiGate I Security    2. NSE4 - FortiGate II Infrastructure    3. NSE5 – FortiAnalyzer    4. NSE6 – FortiAuthenticator    5. NSE6 – FortiMail    6. NSE7 - FortiGate III Enterprise Firewall    7. NSE7 – Advanced Threat Protection Atp   ważne przez okres co najmniej 18 miesięcy w autoryzowanym ośrodku szkoleniowym na terenie Warszawy. | | | | |

Zamawiający dopuszcza dostarczenie produktów równoważnych tworzących klaster HA o poniższych parametrach technicznych (wraz z przeniesieniem konfiguracji obecnie eksploatowanych urządzeń Fortigate 600C):

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Tryb pracy** | System realizujący funkcję Firewalla pracującego w układzie HA musi dawać możliwość pracy w jednym z trzech trybów:   1. Routera z funkcją NAT, 2. Transparentnym 3. Monitorowania na porcie SPAN. |
| **1** | **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu bezpieczeństwa pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia urządzeń w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. System bezpieczeństwa musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. System bezpieczeństwa musi monitorować stan realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
| **2** | **Interfejsy, dysk, zasilanie** | 1. System realizujący funkcję Firewall musi dysponować minimum: 2. 8 portami Gigabit Ethernet RJ-45. 3. 8 gniazdami SFP 1 Gbps. 4. 2 gniazdami SFP+ 10 Gbps. 5. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 6. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 4000 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 7. System musi być wyposażony w zasilanie AC (dwa redundantne zasilacze – hot-swappable) . |
| **3** | **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 8 mln jednoczesnych połączeń oraz 450.000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniejsza niż 36 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniejsza niż 27 Gbps dla pakietów 64 B. 4. Przepustowość Firewall z włączoną funkcją kontroli aplikacji: nie mniejsza niż 15Gbps. 5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 20 Gbps. 6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu - minimum 10 Gbps. 7. Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps. 8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8 Gbps. |
| **4** | **Funkcje Systemu Bezpieczeństwa:** | W ramach dostarczonego systemu bezpieczeństwa należy realizować wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   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. Analiza ruchu szyfrowanego protokołem SSL. 11. Analiza ruchu szyfrowanego protokołem SSH. |
| **5** | **Polityki, Firewall** | 1. Polityki Firewalla muszą 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: 3. Translację jeden do jeden oraz jeden do wielu. 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu bezpieczeństwa musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
| **6** | **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: 2. Wsparcie dla IKE v1 oraz v2. 3. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM). 4. Obsługa protokołu Diffie-Hellman grup 19 i 20. 5. Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. 6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 9. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. 10. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 11. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: 12. 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. 13. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |
| **7** | **Routing i obsługa łączy WAN** | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: 2. Routingu statycznego, 3. Policy Based Routingu,Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 4. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |
| **8** | **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. |
| **9** | **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. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
| **10** | **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Ochrana 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. |
| **11** | **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. |
| **12** | **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. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 4. 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. 5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |
| **13** | **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: 2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 4. Haseł dynamicznych (np.:RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 5. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 6. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On (SSO) przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| **14** | **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. |
| **15** | **Logowanie** | 1. System musi mieć możliwość logowania do systemu logowania i raportowania dostarczonego w ramach postępowania. 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. 5. System zabezpieczeń firewall musi posiadać wbudowane dwa twarde dyski do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB. |
| **16** | **Wirtualizacja** | W ramach dostarczonego systemu bezpieczeństwa (klaster HA urządzeń firewall) musi być zapewniona możliwość budowy minimum 10 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. System musi wspierać IPv4 oraz IPv6 w zakresie:   1. Firewalla 2. Ochrony w warstwie aplikacji. 3. Protokołów routingu dynamicznego. |
| **17** | **Serwisy i licencje** | W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów oraz obejmować co najmniej:   1. Kontrola Aplikacji, 2. IPS, 3. Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), 4. Analiza typu Sandbox, 5. Antyspam, 6. Web Filtering, 7. bazy reputacyjne adresów IP/domen. |

# **Odnowienie usługi serwisowej dla urządzenia FortiAuthenticator 200D.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L.p.** | **Nazwa urządzenia** | **Numer seryjny** | **Data rozpoczęcia serwisu [dzień-miesiąc-rok]** | **Typ serwisu** | **Miejsce instalacji** |
| **1** | **FortiAuthenticator 200D** | **FAC2HD3A15000071** | 2019-12-17 | Zgodnie z ofertą Wykonawcy | Prokuratura Krajowa  ul. Rakowiecka 26/30  Warszawa |
| **2** | **Inne wymagania** | 1. Wykonawca zapewni serwis pogwarancyjny realizowany przez producenta rozwiązania lub Autoryzowanego Dystrybutora producenta. 2. Wykonawca zapewni dostęp wskazanego personelu Zamawiającego do dedykowanego portalu www producenta urządzenia, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do bazy wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp.. 3. Wykonawca zapewni możliwość zgłaszania na stronach www producenta sprzętu problemów eksploatacyjnych związanych z obsługą sprzętu będącego przedmiotem zamówienia. 4. Zaproponowany pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (nie tylko do serwisu Wykonawcy) przez cały okres świadczenia usług serwisowych. 5. Wykonawca w oferowanych pakietach serwisowych producenta zapewni dostęp do pomocy technicznej producenta (drogą telefoniczną, poprzez email lub stronę WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego. 6. **W ramach realizacji umowy Wykonawca dokona wymiany obecnie eksploatowanego urządzenia FortiAuthenticator 200D na urządzenie FortiAuthenticator 200E posiadający wszystkie licencje i subskrypcje jak dotychczas wykorzystywane rozwiązanie oraz zapewni dostęp do najnowszego oprogramowania i sygnatur do urządzenia objętego serwisem. Wykonawca będzie świadczył usługi serwisu gwarancyjnego dla tak dostarczonych urządzeń na warunkach określonych w umowie. Wykonawca dokona migracji konfiguracji z obecnie eksploatowanego rozwiązania do docelowego.** 7. **Wykonawca dostarczy 600 sztuk tokenów sprzętowych FTK-200 zgodnych z dostarczanym rozwiązaniem.** | | | | |

Zamawiający dopuszcza dostarczenie urządzenia równoważnego spełniającego co najmniej poniższe wymagania techniczne (wraz z przeniesieniem konfiguracji obecnie eksploatowanych urządzeń FortiAuthenticator 200D):

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Architektura systemu** | 1. Dostarczony system uwierzytelniania musi zapewniać wszystkie wymienione poniżej funkcje. Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników i ich uwierzytelnianiem. 2. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie pochodziły od jednego producenta. |
| **1** | **System operacyjny** | 1. Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. |
| **2** | **Parametry fizyczne systemu** | 1. System uwierzytelniający musi być dostarczony w postaci maszyny fizycznej.   Urządzenie musi posiadać minimum:   1. dysk o pojemności min. 1TB 2. zasilanie AC 3. 4 interfejsy 10/100/1000 Ethernet RJ45 4. port konsoli szeregowej |
| **3** | **Wymagania ogólne** | System powinien pozwalać na nie mniej niż:   1. Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki, bez konieczności stosowania zewnętrzej konsoli zarządzającej 2. Możliwość pracy w konfiguracji HA (High Availability) 3. Odpytywanie o stan urządzenia w oparciu o protokół SNMP (v1, v2, v3) oraz wykorzystanie SNMP Trap celem monitorowania (nie mniej niż):    1. obciążenia procesor(a/ów)    2. wykorzystania pamięci    3. informacji o osiąganiu granicznej liczby użytkowników    4. informacji o osiąganiu granicznej liczby grup użytkowników    5. informacji o osiąganiu granicznej liczby uwierzytelnionych użytkowników    6. przekroczeniu ilości uwierzytelnień    7. przekroczeniu ilości błędnych uwierzytelnień 4. Graficzną reprezentację statusu uwierzytelnień 5. Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia i nazwy użytkownika:    1. lokalnie    2. zdalnie w oparciu o protokół Syslog 6. Aktualizację systemu operacyjnego z poziomu graficznego interfejsu zarządzającego (GUI) 7. Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI)    1. również w oparciu o harmonogram w cyklu godzinowym, dziennym, tygodniowym lub miesięcznym wraz z określaniem godzin i minut    2. rzeczona kopia bezpieczeństwa może być również zapisywana przy pomocy protokołu FTP/SFTP 8. Konfigurację captive portal |
| **4** | **Wymagania funkcjonalne - uwierzytelnianie** | Celem realizacji funkcji uwierzytelniających, system powinien wspierać nie mniej niż:   1. Lokalną, wbudowaną bazę użytkowników wraz z możliwością wykonywania nie mniej niż następujących akcji na użytkowniku: tworzenie, przypisanie tokena i zarządzanie nim, blokowanie konta (locking), usuwanie. 2. Przechowywanie następujących informacji o użytkowniku: nazwa (username), imię/nazwisko, adres email, numer telefonu komórkowego, numer telefonu, adres, kraj, stan/województwo. 3. Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV. 4. Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:    1. poziomu złożoności hasła (jego długości minimalnej, cyfr i znaków specjalnych),    2. czasu życia hasła,    3. możliwości ponownego użycia tych samych haseł. 5. Konfigurowalną politykę blokowania kont:    1. w oparciu o ilość nieudanych logowań,    2. czas blokowania,    3. okres nieaktywności, po którym konto jest blokowane. 6. Uruchomienie portalu do samodzielnej rejestracji użytkowników:    1. opcjonalnie tworzenie ich kont może wymagać akceptacji administratora,    2. wymagana jest również opcja tworzenie kont bez ingerencji administratora. 7. Obsługę protokołu RADIUS zgodną z RFC:    1. wbudowany serwer RADIUS,    2. konfiguracja serwera pozwala na ograniczenie dostępu tylko do wskazanych urządzeń NAS,    3. integrację z zewnętrznymi serwerami RADIUS. 8. Obsługę protokołu LDAP:    1. wbudowany serwer LDAP,    2. możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP). 9. Obsługę SAML. 10. Realizacje funkcjonalności SSO (Single Sign On) w oparciu o:     1. integrację z Active Directory również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny,     2. dedykowaną aplikację na stacje robocze z systemem Windows,     3. RADIUS,     4. informacje uzyskiwane poprzez protokół Syslog,     5. dedykowany portal. |
| **5** | **Wymagania funkcjonalne - uwierzytelnianie dwuskładnikowe** | Realizując uwierzytelnianie dwuskładnikowe, system musi spełniać nie mniej niż:   1. Obsługę dla tokenów sprzętowych (hardware). Tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania. 2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile. 3. Dla tokenów na system iOS i Android wymaga się:    1. aktywacji z centralnego systemu uwierzytelniania (seed provisioning),    2. generowania kodu (cyfr) co 30 lub 60 sekund,    3. możliwości dezaktywacji tokena oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),    4. ochrony dostępu poprzez konfigurowalny kod PIN,    5. aktywacji w oparciu o kod QR. 4. Możliwość dostarczenia kodu (wskazania tokena) poprzez:    * 1. email (wygaśnięcie kodu w czasie 10-3600 sekund),      2. SMS (wygaśnięcie kodu w czasie 10-3600 sekund),      3. konfiguracja bramki SMS w oparciu o HTTP/S i/lub SMTP. 5. W przypadku tokenów programowych możliwość wykorzystania notyfikacji push przychodzących na urządzenie mobilne i zawierających szczegóły dotyczące żądania logowania w celu zaakceptowania ich jednym "kliknięciem". 6. Możliwość integracji z logowaniem do systemu Windows. 7. Wsparcie dla API. |
| **6** | **Wymagania funkcjonalne - 802.1x** | System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:   1. dla sieci bezprzewodowych wymagane są następujące protokoły:    1. PEAP,    2. EAP-TTLS,    3. EAP-TLS,    4. EAP-GTC, 2. wsparcie dla uwierzytelniania w oparciu o adres MAC (MAC based authentication), 3. zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTL, TLS EAP. |
| **7** | **Wymagania funkcjonalne - zarządzanie certyfikatami** | System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:   1. własne, samodzielne CA (Certificate Authority), 2. CA pośredniczące (intermediary CA), 3. ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego, 4. możliwość pobrania wygenerowanych certyfikatów, 5. możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP, 6. możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP, 7. realizacja CRL (Certificate Revocation List), 8. wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560). |
| **8** | **Parametry wydajnościowe i licencyjne** | Urządzenie musi obsługiwać co najmniej:   1. uwierzytelnianie dla nie mniej niż 500 użytkowników, 2. 1000 tokenów (uwierzytelnianie dwuskładnikowe), 3. 160 klientów protokołu RADIUS (urządzeń NAS), 4. 50grup użytkowników, 5. 10 certyfikatów głównych (CA), 6. 2000 certyfikatów użytkowników. 7. Wraz z urządzeniem należy dostarczyć 600 tokenów sprzętowych poprawnie współpracujących z dostarczanym rozwiązaniem. |
| **9** | **Zarządzanie** | System udostępnia co najmniej graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. |

# **Odnowienie usługi serwisowej dla urządzenia FortiAnalyzer 1000D.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L.p.** | **Nazwa urządzenia posiadanego przez Zamawiającego** | **Numer seryjny** | **Data rozpoczęcia serwisu [dzień-miesiąc-rok]** | **Typ serwisu** | **Miejsce instalacji** |
| **1** | **FortiAnalyzer 1000D** | **FL-1KD3A13000077** | 2020-12-31 | Zgodnie z ofertą Wykonawcy | Prokuratura Krajowa  ul. Rakowiecka 26/30  Warszawa |
| **2** | **Inne wymagania** | 1. Wykonawca zapewni serwis pogwarancyjny realizowany przez producenta rozwiązania lub Autoryzowanego Dystrybutora producenta. 2. Wykonawca zapewni dostęp wskazanego personelu Zamawiającego do dedykowanego portalu www producenta urządzenia, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do bazy wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego itp.. 3. Wykonawca zapewni możliwość zgłaszania na stronach www producenta sprzętu problemów eksploatacyjnych związanych z obsługą sprzętu będącego przedmiotem zamówienia. 4. Zaproponowany pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (nie tylko do serwisu Wykonawcy) przez cały okres świadczenia usług serwisowych. 5. Wykonawca w oferowanych pakietach serwisowych producenta zapewni dostęp do pomocy technicznej producenta (drogą telefoniczną, poprzez email lub stronę WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego. 6. **W ramach realizacji umowy Wykonawca dokona wymiany obecnie eksploatowanego urządzenia FortiAnalyzer 1000D na urządzenie FortiAnalyzer 3000F posiadający wszystkie licencje i subskrypcje jak dotychczas wykorzystywane rozwiązanie oraz zapewni dostęp do najnowszego oprogramowania i sygnatur do urządzenia objętego serwisem. Wykonawca będzie świadczył usługi serwisu gwarancyjnego dla tak dostarczonych urządzeń na warunkach określonych w umowie. Wykonawca dokona migracji konfiguracji z obecnie eksploatowanego rozwiązania do docelowego.** 7. Wraz z urządzeniem Wykonawca dostarczy licencję FortiGuard Indicator of Compromise (IOC) Subscription na cały okres obowiązywania umowy. | | | | |

Zamawiający dopuszcza dostarczenie urządzenia równoważnego spełniającego co najmniej poniższe wymagania techniczne (wraz z przeniesieniem konfiguracji obecnie eksploatowanych urządzeń FortiAnalyzer 1000D):

lub rozwiązanie równoważne o poniższych parametrach:

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

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Platforma** | 1. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej wraz z odpowiednio zabezpieczonym systemem operacyjnym |
| **1** | **Interfejsy, dysk, zasilanie:** | 1. System musi dysponować co najmniej: 2. 4 portami Gigabit Ethernet RJ-45. 3. 2 gniazdami SFP+ 10 Gbps. 4. Rozwiązanie musi dysponować powierzchnią dyskową min. 48 TB. 5. 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 0, 1, 5, 6,10, 50, 60. |
| **2** | **Parametry wydajnościowe:** | 1. System musi być w stanie przyjmować minimum 3 TB logów na dzień. 2. System musi być w stanie przeanalizować minimum 40000 logów na sekundę. 3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 100 systemów. |
| **3** | **Logowanie** | W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:   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: 4. Listę najczęściej wykrywanych ataków. 5. Listę najbardziej aktywnych użytkowników. 6. Listę najczęściej wykorzystywanych aplikacji. 7. Listę najczęściej odwiedzanych stron www. 8. Listę krajów, do których nawiązywane są połączenia. 9. Listę najczęściej wykorzystywanych polityk Firewall. 10. Informacje o realizowanych połączeniach IPSec. 11. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 12. 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. 13. System musi realizować cykliczny eksport logów do zewnętrznego systemu. 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 tworzenia raportów w języku polskim. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres(y) 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: 4. Malware. 5. Aplikacje sieciowe. 6. Email. 7. IPS. 8. Traffic. 9. 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 dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 2. 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** | **Dodatkowe licencje** | 1. Licencja Indicators of Compromise (IoC) |

# **Zakup licencji oprogramowania Endpoint Protection na stacje PC z systemem Windows w pełni współpracującego z urządzeniami bezpieczeństwa posiadanymi przez Zamawiającego.**

Oprogramowanie Endpoint Protection na urządzenia końcowe z systemem Windows oraz Mac OS chroniące przed zagrożeniami – nazywane dalej „Klientem”. Oprogramowanie musi zostać dostarczone dla 1000 urządzeń końcowych i objęte będą wsparciem producenta od dnia podpisania umowy.

|  |  |  |
| --- | --- | --- |
| **L.p.**  **1** | **Oprogramowanie Endpoint Protection** | 1. Klient musi wspierać system operacyjny Windows oraz Mac OS. 2. Klient musi posiadać następujące funkcjonalności bezpieczeństwa:    1. Antywirus    2. Web Filtering    3. Kontrola aplikacyjna    4. IPSec VPN oraz SSL VPN    5. Patch management – instalacja dostępnych łat dla oprogramowania zainstalowanego na urządzeniach końcowych, np. przeglądarek internetowych. 3. Dla systemu Windows rozwiązanie musi posiadać integrację z systemem Sandbox tego samego producenta. Integracja musi umożliwiać wysłanie pliku do przeskanowania w systemie sandbox i jednoczesne umieszczenie pliku w tymczasowej „kwarantannie” – użytkownik może uzyskać dostęp do pliku po otrzymaniu przez Klienta odpowiedzi od systemu sandbox, że plik nie nosi znamion pliku niebezpiecznego. 4. Wymagane jest dostarczenie oprogramowania umożliwiającego centralne zarządzanie wszystkimi Klientami, w tym między innymi:    1. Instalacja oraz aktualizacja Klienta na wybranych komputerach    2. Integracja z Windows AD umożliwiająca m.in. uzyskanie informacji o wykorzystywanych urządzeniach z systemem Windows oraz grupach AD.    3. Inwentaryzacja oprogramowania na urządzeniach z zainstalowanym Klientem.    4. Informacje o zagrożeniach wykrytych na poszczególnych urządzeniach.    5. Centralne tworzenie polityk bezpieczeństwa przypisywanych grupom użytkowników.    6. Zdalne uruchamianie skanowania danego urządzenia oraz instalacji łat oprogramowania zainstalowanego na urządzeniu.    7. Telemetria 5. **Klient musi umożliwiać integrację z zaporami ogniowymi (firewall) tego samego producenta co urządzenia wskazane pkt I. w zakresie:**    1. Sprawdzanie zgodności urządzeń końcowych z polityką bezpieczeństwa – tylko urządzenia z zainstalowanym Klientem i z określonym ustawieniem profili bezpieczeństwa Klienta, mogą uzyskać dostęp do Internetu za pośrednictwem firewall.    2. Przekazywanie przez Klienta dodatkowych informacji do zapory ogniowej na temat urządzenia końcowego, w tym nazwa zalogowanego użytkownika, informacje o systemie operacyjnym, adres IP, informacje o wykrytych przez Klienta zagrożeniach na tym urządzeniu.    3. Możliwość automatycznego zablokowania dostępu do wszystkich sieci już na poziomie Klienta, tzn. także komunikacji z urządzeniami znajdującymi się w tej samej domenie rozgłoszeniowej L2 modelu OSI, w wyniku podejrzanych aktywności wykrytych przez zintegrowane fizyczne urządzenia firewall. |

# **Zakup rozwiązania do analizy i wykrywania zaawansowanych i nieznanych zagrożeń za pomocą technologii „Sandbox” współpracującego z oprogramowaniem Endpoint Protection jak i urządzeniami bezpieczeństwa eksploatowanymi przez Zamawiającego.**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Architektura systemu** | 1. Elementy systemu powinny zostać dostarczone w postaci komercyjnej platformy (lub komercyjnych platform) sprzętowej. 2. System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji. 3. System powinien umożliwiać lokalne logowanie i raportowanie oraz współpracować z systemem centralnego logowania i raportowania. 4. Musi istnieć możliwość implementacji systemu w trybie nasłuchu oraz współpracy z systemami zabezpieczeń NGFW (Next Generation Firewall) lub SWG (Security Web Gateway), SEG (Secure Email Gateway) oraz w oparciu o interfejsy programistyczne API. 5. Dla zapewnienia szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcie i aktualizacje oprogramowania. 6. System powinien mieć możliwość pracy w konfiguracji HA (High Availability) z podziałem obciążenia. |
| **1** | **System operacyjny** | 1. Dla zapewnienia wysokiej sprawności i skuteczności działania elementy systemu muszą pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. |
| **2** | **Parametry fizyczne systemu** | 1. System musi dysponować minimum: 2. 4 portami Gigabit Ethernet RJ-45. 3. 4 gniazdami SFP 1 Gbps. 4. Powierzchnia dyskowa - minimum 2 TB. 5. Redundantne zasilanie z sieci 230V/50Hz. |
| **3** | **Parametry wydajnościowe** | 1. System musi pozwalać na analizę w maszynach wirtualnych min. 280 plików na godzinę. 2. System musi pozwalać na skanowanie antywirusowe min. 5000 plików na godzinę. 3. System musi zapewniać możliwość uruchomienia min. 14 jednoczesnych instancji (jednoczesna analiza 14 różnych próbek w ramach „pełnego sandboxingu”) maszyn wirtualnych. 4. System musi realizować jednoczesną analizę próbek na obrazach/maszynach wirtualnych następujących systemów operacyjnych: 5. MS Office 6. Windows 7 7. Windows 8 8. Windows 10 |
| **4** | **Funkcje podstawowe i uzupełniające** | 1. System musi umożliwiać „pełny sanboxing”, tzn. wykonanie w maszynie wirtualnej dla następujących rodzajów próbek znajdujących się w wiadomościach pocztowych: adres URL, dokumenty Microsoft Office, pliki wykonywalne (w tym języki skryptowe JavaScript, Visual Basic, PowerShell, bat), pliki PDF (Adobe Acrobat), pliki SWF (Adobe Flash). 2. System 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 3. Funkcjonalność Sandbox dla instancji Windows: sprawdzanie procesów i rejestru, połączenia z Botnet C&C oraz złośliwymi URL, dostęp do pakietów przeprocesowanych przez VM, logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM. 4. Procesowanie plików o rozmiarze co najmniej 8 MB. 5. Sanboxing dla plików zarchiwizowanych (.tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR). 6. Sandboxing plików multimedialnych: .avi, .mpeg, .mp3, .mp4. 7. Skanowanie stron www z linkami URL. 8. Czarne i białe listy dla sum kontrolnych plików. 9. Szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci, snapshotu VM. Administrator powinien mieć możliwość definiowania cyklicznych raportów. 10. Dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap. 11. System musi umożliwiać generowanie alertów podczas wykrywania zagrożeń i raportowanie ich za pomocą: Syslog, SNMP, SMTP. 12. System musi umożliwiać zarządzanie min. przez panel WebUI za pomocą przeglądarki internetowej. |
| **5** | **Sygnatury, subskrypcje** | 1. Bazy sygnatur wykorzystywanych przez funkcje skanujące powinny być systematycznie aktualizowane. 2. W ramach postępowania zostaną dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji skanujących oraz analitycznych |