*Załącznik nr 2 do Zaproszenia – Specyfikacja techniczna i warunki gwarancji*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Nazwa i adres Wykonawcy*

*(stempel firmowy)*

Postanowienia ogólne, dotyczące:

**części 1, 2 i 3:**

1. Dostarczane urządzenia i oprogramowanie są fabrycznie i technicznie nowe i nie używane wcześniej.
2. Urządzenia posiadają certyfikat zgodności z Dyrektywami Nowego Podejścia UE (urządzenia muszą być oznaczone symbolem CE).
3. Urządzenia i oprogramowanie pochodzą z legalnego kanału sprzedaży.
4. Dostarczane urządzenia/oprogramowanie są pozbawione wszelkich wad.
5. Wszystkie oferowane urządzenia w ramach poszczególnych typów są:

• złożone z identycznych podzespołów, sygnowanych przez ich producenta,

• posiadają taką samą konfigurację,

• dostarczane są w oryginalnych opakowaniach.

**części 3:** Zamawiający będzie wymagał oświadczenia producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

|  |  |  |
| --- | --- | --- |
| **CZĘŚĆ 1 \*** | | |
| **Komputer klasy PC typu AIO HP 800 G6 lub równoważny - 3 szt.** | | |
| **Cecha** | **Wymagane minimalne parametry techniczne** | **Zaoferowane urządzenie**  **Nazwa** (typ/model) **………….. Producent ……………….**  **Parametry** (podać dokładne parametry) |
| Ekran | Matryca IPS WLED. Rozmiar matrycy 24”, rozdzielczość natywna matrycy FHD 1920x1080, kąty widzenia matrycy pionowo: 178 stopni, poziomo 178 stopni. |  |
| Procesor | Procesor Intel Core i5-10500 lub równoważny osiągający w teście PassMark CPU Mark średni wynik 13291 punktów. |  |
| Pamięć RAM | 8 GB SODIMM DDR4, wolny jeden slot do rozbudowy pamięci, rozbudowa do 64GB |  |
| Dysk twardy | 256GB SSD |  |
| Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu. |  |
| Wyposażenie multimedialne | Karta dźwiękowa 2 kanałowa zintegrowana z płytą główną, zgodna  z High Definition, wbudowane dwa głośniki 2W na kanał.  Wbudowana w obudowę matrycy cyfrowa kamera 5.0 MP, rozdzielczość video min. 1920x1080. Kamera opatrzona w inny system.  Dwa cyfrowe mikrofony obsługujące poprawę mowy i redukcję szumów |  |
| Porty | Wbudowane:  7xUSB 3.1, w tym 2 porty USB 3.1 gen 2 typu C. 1xRJ45 (zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE , 1x DisplayPort out, 1 x HDMI in, 1x audio combo.  Wszystkie porty wyprowadzone na zewnątrz obudowy. |  |
| Klawiatura | Klawiatura bezprzewodowa w układzie polski programisty w kolorze zbliżonym do koloru obudowy. |  |
| Mysz | Mysz optyczna bezprzewodowa w kolorze zbliżonym do koloru obudowy. |  |
| Obudowa | Typu All-in-One, w której komponenty takie jak matryca, zasilacz, płyta główna, procesor, pamięć RAM oraz dysk twardy są zintegrowane w jednej obudowie.  Obudowa umożliwia zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona ). Blokada uniemożliwia otwarcie obudowy.  Demontaż standu odbywa się bez użycia narzędzi, mocowanie standu opatrzone w przycisk zwalniający. Demontaż tylnej pokrywy odbywa się również bez użycia narzędzi,  Każdy komputer oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie oraz wpisanym na stałe w BIOS.  Zasilacz wewnętrzny o mocy 200W pracujący w sieci 230V 50/60Hz prądu zmiennego.  Obudowa posiada czujnik otwarcia obudowy współpracujący  z oprogramowaniem zarządzająco – diagnostycznym.  funkcjonalność stand’u :  - zakres pochyłu 35 stopni, przód -5 , tył 30 stopni,  - regulacja wysokości 10cm  - pivot |  |
| Płyta główna | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia |  |
| Bezpieczeństwo | Czujnik otwarcia obudowy.  Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności: testy uruchamiane automatycznie lub w trybie interaktywnym, możliwość powtórzenia testów. podsumowanie testów z możliwością zapisywania wyników, uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu. Uruchamianie testów zdefiniowanych przez użytkownika, wyświetlanie wiadomości, które informują o stanie przeprowadzanych testów, wyświetlanie wiadomości o błędach, które informują o problemach napotkanych podczas testów. Test musi zawierać informację o nazwie komputera, wersji BIOS, numerze seryjnym komputera. Podawać dokładne informacje o wszystkich zainstalowanych komponentach, a w szczególności zawierać informacje o numerze seryjnym, typie i pojemności dysku twardego, informacji o obrotach wentylatora CPU, informacji o procesorze w tym model i taktowanie, informacji o pamięci w tym wielkość podana w MB, obsadzenie w konkretnym banku, typ pamięci wraz z taktowaniem oraz SN i PN, wykaz temperatur CPU, pamięci, temperatury panującej wewnątrz. System działający nawet w przypadku braku dysku twardego, jego uszkodzenia, bez dostępu do internetu i sieci lokalnej pozwalający na uzyskanie wyżej wymienionych funkcjonalności a w szczególności na przetestowanie: procesora i pamięci (procedura POST traktowane jest jako oddzielny system diagnostyczny – wizualny świetlny system). Nie dopuszcza się stosowanie pomocy zewnętrznych w celu uzyskania pełnej funkcjonalności (np. pamięć USB itp.) |  |
| Bios | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera.  Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych, odczytania z BIOS informacji o: dacie produkcji komputera (data produkcji nieusuwalna), kontrolerze audio, procesorze (w szczególności min. i max. osiągana prędkość), pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej  z zewnętrznych urządzeń.  Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.  Funkcja logowania się do BIOS na podstawie hasła użytkownika, administratora (hasła niezależne).  Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. |  |
| System operacyjny | Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego lub z partycji recovery.  Zamawiający dopuszcza rozwiązanie równoważne spełniające następujące wymagania:  System musi mieć możliwość dodania do domeny opartej na systemie Windows 2019.  System musi mieć możliwość zarządzania przez polisy GPO oparte  o domenę na Windows 2019.  System musi pozwalać na zarządzanie z poziomu konsoli users and computers z kontrolera domeny opartego na systemie Windows 2019 - dotyczy to zarządzania użytkownikami, grupami oraz przeglądania logów.  System będzie stosował polityki bezpieczeństwa z polis GPO opartych o domenę Windows 2019.  System musi mieć możliwość użycia filtrów WMI w celu zbierania informacji, stosowanie filtrów musi być możliwe przez polisy GPO oparte o domenę na systemie Windows 2019.  System musi umożliwić zainstalowanie aplikacji MS Office bez użycia aplikacji wirtualizujących środowisko Windows. |  |
| Certyfikaty | 1. Certyfikat ISO 9001 dla producenta sprzętu. 2. Certyfikat TCO dla oferowanego modelu AIO, potwierdzenie spełnienia musi znajdować się na liście opublikowanej na stronie : http://tcocertified.com. – 3. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 4. Komputer spełnia wymogi normy Energy Star 6.0.   wpis dotyczący oferowanego komputera w internetowym katalogu <http://www.eu-energystar.org> lub <http://www.energystar.gov>. |  |
| Gwarancja | **3-letnia gwarancja** producenta świadczona w miejscu instalacji sprzętu.  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Serwis urządzeń realizowany przez Autoryzowanego Partnera Serwisowego Producenta. |  |

|  |  |  |
| --- | --- | --- |
| **c.d. Część 1 \*** | | |
| **Laptop Dell Latitude 3510 lub równoważny – 5 szt.** | | |
| **Cecha** | **Wymagane minimalne parametry techniczne** | **Zaoferowane urządzenie**  **Nazwa** *(typ/model)* **………….. Producent ……………….**  **Parametry** *(podać dokładne parametry)* |
| Ekran | Matryca rozmiar matrycy w przedziale 15,6”, rozdzielczość natywna matrycy FHD 1920x1080. Matryca z powłoką antyrefleksyjną |  |
| Procesor | Procesor Intel Core i5-10210U lub równoważny osiągający w teście PassMark CPU Mark średni wynik 6507 punktów. |  |
| Pamięć RAM | 8 GB SODIMM DDR4, rozbudowa do 32GB. Dwa sloty pamięci, 1 slot wolny. |  |
| Dysk twardy | 256GB SSD. |  |
| Wyposażenie multimedialne | Karta dźwiękowa 2 kanałowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane dwa głośniki.  Mikrofon z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.  Kamera internetowa trwale zainstalowana w obudowie matrycy.  Wi-Fi  Bluetooth |  |
| Porty | Wbudowane:  - 3xUSB 3.1,  - 1xRJ45 ( zintegrowana z płytą główną),  - 1x HDMI,  - audio combo.  - gniazdo zasilania notebooka. |  |
| Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu. |  |
| Bateria i zasilanie | Bateria czterokomorowa o pojemności 53Whr. Zasilacz o mocy 65W. |  |
| Waga i wymiary | 1,79 kg z baterią 4 cell.  Suma wymiarów notebooka nie większa niż 564mm. |  |
| Diagnostyka | System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku. |  |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag. Funkcje logowania się do BIOS na podstawie hasła użytkownika, administratora (hasła niezależne), informację o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS.  Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. |  |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. |  |
| Klawiatura | Klawiatura w układzie polski programisty |  |
| Zasilacz | Dedykowany sygnowany logiem producenta oferowanego laptopa |  |
| Mysz | Mysz bezprzewodowa sygnowana logiem producenta oferowanego laptopa |  |
| System operacyjny | Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego lub z partycji recovery.  Zamawiający dopuszcza rozwiązanie równoważne spełniające następujące wymagania:  System musi mieć możliwość dodania do domeny opartej na systemie Windows 2019.  System musi mieć możliwość zarządzania przez polisy GPO oparte  o domenę na Windows 2019.  System musi pozwalać na zarządzanie z poziomu konsoli users and computers z kontrolera domeny opartego na systemie Windows 2019 - dotyczy to zarządzania użytkownikami, grupami oraz przeglądania logów.  System będzie stosował polityki bezpieczeństwa z polis GPO opartych o domenę Windows 2019.  System musi mieć możliwość użycia filtrów WMI w celu zbierania informacji, stosowanie filtrów musi być możliwe przez polisy GPO oparte o domenę na systemie Windows 2019.  System musi umożliwić zainstalowanie aplikacji MS Office bez użycia aplikacji wirtualizujących środowisko Windows. |  |
| Torba | Dedykowana, sygnowana logiem producenta oferowanego laptopa |  |
| Certyfikaty | Certyfikat ISO 9001  Komputer spełnia wymogi normy Energy Star 6.0  wpis dotyczący oferowanego komputera w internetowym katalogu <http://www.eu-energystar.org> lub <http://www.energystar.gov>.  Certyfikat TCO, certyfikacja na stronie : <https://tcocertified.com/product-finder/> – załączyć do oferty wydruk z strony. |  |
| Gwarancja | **3-letnia gwarancja** producenta świadczona w miejscu instalacji sprzętu.  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Serwis urządzeń musi być realizowany przez producenta lub Autoryzowanego Partnera Serwisowego Producenta. |  |

|  |  |  |
| --- | --- | --- |
| **CZĘŚĆ 2 \*** | | |
| **Serwer NAS Qnap TS-877XU-RP z wyposażeniem lub równoważny – 1 szt.** | | |
| **Cecha** | **Wymagane minimalne parametry techniczne** | **Zaoferowane urządzenie**  **Nazwa** *(typ/model)* **………….. Producent ……………….**  **Parametry** *(podać poniżej dokładne parametry)* |
| Typ urządzenia | Serwer NAS w obudowie typu rack |  |
| Procesor | AMD Ryzen™ 5 3600 lub Intel Xeon lub równoważny |  |
| Pamięć systemowa | 16 GB UDIMM DDR4 2400 MHz (2 x 8GB) |  |
| Wnęka dysków | 8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s |  |
| Kompatybilność dysków | 3,5-calowe dyski twarde SATA  2,5-calowe dyski twarde SATA  2,5-calowe dyski SSD SATA |  |
| Obsługa przyspieszenia pamięci podręcznej SSD | Tak |  |
| Port Gigabit sieci Ethernet (RJ45) | Min. 2 porty 1GbE zintegrowane |  |
| Port 10 Gigabit sieci Ethernet | Min. 2 porty 10GbE SFP+ |  |
| Gniazdo PCIe | Min. 4 gniazda PCIe Gen3 x4 |  |
| Port USB 3.2 Gen 1 | Min. 2 porty |  |
| Port USB 3.2 Gen 2 (10 Gb/s) | Min. 2 porty |  |
| Kształt | 2U, do montażu stelażowego w szafie rack |  |
| Zasilacz | Min. 2 zasilacze po 300W, 100-240V |  |
| Obsługa RAID | Min. RAID 50/60, RAID 10, RAID 6, RAID 5. |  |
| Uwierzytelnianie Microsoft Active Directory (AD) | Tak |  |
| Obsługa w języku polskim | Tak |  |
| **Wyposażenie dodatkowe** | - 8 szt. dysków twardych WD Red Pro 4TB,  - karta rozszerzeń QM2-2P-344 zapewniająca obsługę dysków M.2 SSD,  - 2 szt. dysków M.2 SSD min. 256GB każdy kompatybilne z proponowanym urządzeniem,  - karta QXG-10G1T,  - szyny do montażu w szafie rack RAIL-B02 ,  - 2 szt. kable SFP+ 10GbE twinaxial direct attach. |  |
| Gwarancja | Serwis urządzeń musi być świadczony w miejscu instalacji sprzętu, przez producenta sprzętu lub Autoryzowanego Partnera Serwisowego Producenta przez okres **min. 5 lat**. |  |

|  |  |  |
| --- | --- | --- |
| **CZĘŚĆ 3 \*** | | |
| **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 3 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:  • Firewall.  • Ochrony w warstwie aplikacji.  • Protokołów routingu dynamicznego. | | |
| **System bezpieczeństwa (firewall) Fortinet Fortigate 80F lub równoważny – 1 szt.** | | |
| **Cecha** | **Wymaganie** | **Zaoferowane urządzenie**  **Nazwa** *(typ/model)* **………….. Producent ……………….**  **Parametry** *(podać poniżej dokładne parametry)* |
| 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:  • 8 portami Gigabit Ethernet RJ-45.  • 2 gniazdami SFP 1 Gbps.  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.  4. System musi być wyposażony w zasilanie AC. |  |
| Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.  2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.  3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.  4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.  5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.  6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.  7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 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 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.  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. |  |
| 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.  3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  4. 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  • Cisco ACI.  • Google Cloud Platform (GCP).  • OpenStack.  • VMware vCenter (ESXi). |  |
| 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.  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. |  |
| 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. |  |
| 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 Safe Search – 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 ulr - 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. |  |
| 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.  1. 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.  2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.  3. 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 5 lat. |  |
| Gwarancja oraz wsparcie | System musi być objęty **serwisem gwarancyjnym producenta przez okres 5 lat**, 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. |  |

*\* niepotrzebne skreślić*

Miejscowość i data…………………….......................

Imię, nazwisko osoby podpisującej…………………………………….…Podpis dokumentu………...

*(Podpis osoby lub osób uprawnionych do reprezentowania wykonawcy w dokumentach rejestrowych lub we właściwym pełnomocnictwie).*