***Załącznik nr 5 do SWZ***

**ZNAK SPRAWY: GK.271.17.2022**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Dostawa sprzętu komputerowego w ramach zadania pn.:** **Realizacja projektu grantowego „Cyfrowa Gmina”**

* + - 1. **LOKALIZACJA.**

Urząd Miejski w Lidzbarku Warmińskim, ul. Świętochowskiego 14 , 11-100 Lidzbark Warmiński.

* + - 1. **OGÓLNE WARUNKI DOSTAWY SPRZĘTÓW INFORMATYCZNYCH.**

1. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego
2. Wykonawca zapewni transport sprzętów na miejsce ich instalacji.
3. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nie noszący oznak użytkowania.
4. Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
5. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta.
6. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
7. Urządzenie na etapie dostawy producent a zamawiający nie mogą podlegać modyfikacjom.
8. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji w dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
9. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
10. Prace instalacyjne należy realizować w dni robocze w godzinach pracy Zamawiającego, w ustaleniu z Zamawiającym.
11. Ewentualne odstępstwa mogą być realizowane wyłącznie za zgodą Zamawiającego.
12. Wykonawca jest zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i systemów, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i systemów.
13. Gwarancja i serwis na urządzenia musi być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku gdy Oferent nie posiada takiej autoryzacji.
14. Możliwość sprawdzenia statusu gwarancji dla pełnej konfiguracji oferowanych urządzeń na stronie producenta po podaniu nr seryjnego (jeśli producent oferuje taką możliwość).
15. Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
16. Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.

**CZĘŚĆ 1 – ZESTAWY KOMPUTEROWE ORAZ LAPTOP**

1. **Monitor 39 szt.**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Parametr** | **Wymagania minimalne** |
| **Monitor** | | |
| 1 | Wyświetlacz monitora | Kolorowy 23,8” nie więcej niż 26” (włącznie) , 16:9, Full HD, rozdzielczość fizyczna 1920x1080 przy 60 Hz |
| 2 | Rodzaj ekranu | Matryca matowa z podświetlaniem LED, IPS |
| 3 | Parametry monitora | czas reakcji matrycy – nie więcej niż 5 ms |
| jasność – 250 cd/m2 lub większa |
| kontrast statyczny minimum 1000:1 |
| 4 | Złącza monitora | Złącza cyfrowe zgodnie z oferowanym komputerem bez konieczności stosowania przejściówek |
| 5 | Wbudowane głośniki | Minimum 2x2W |
| 6 | Możliwość regulacji ustawienia monitora | Regulacja kąta pochylenia monitora |
| 7 | Niezawodność / jakość wytwarzania | Potwierdzona certyfikatami:  Certyfikat CE  ISO 14001  ISO 9001 |
| 8 | Kable logiczne | Zgodne z oferowanym komputerem bez konieczności stosowania przejściówek |
| 9 | Zasilanie | 230V ± 10%, 50 Hz, przewód zasilający długości min. 1.8m |
| 10 | Gwarancja | Minimum 24 miesiące licząc od daty podpisania protokołu odbioru końcowego dostaw, wchodzących w zakres przedmiotu zamówienia, wykonanych bez zastrzeżeń  Gwarancja realizowana od daty wystawienia faktury. Usunięcie awarii w ciągu 5 dni roboczych od otrzymania zgłoszenia (przyjmowanie zgłoszeń w dni robocze w godzinach 8.00 - 15.00 telefonicznie, faksem lub e-mail). W przypadku braku możliwości naprawy w w/w terminie nastąpi podstawienie sprzętu zastępczego na czas naprawy o nie gorszych parametrach technicznych. Serwis urządzeń realizowany przez producenta lub autoryzowanego partnera serwisowego producenta na jednakowych warunkach przez cały okres trwania gwarancji.  Wykonawca na własny koszt, w razie potrzeby zapewni transport do i z serwisu. |

1. **Komputer stacjonarny 39 szt.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **L.p.** | **Nazwa elementu,**  **parametru lub cechy** | | | **Wymagania minimalne** |
|  | **Komputer stacjonarny** | | | |
| 1 | Procesor | | Stacja robocza będzie zawierać procesor wielordzeniowy zgodny z architekturą x86 zapewniający możliwość uruchamiania aplikacji 64 bitowych. Zamawiający oczekuje iż zaoferowane urządzenie zawierać będzie procesor umożliwiający uzyskanie minimum **16 300** punktów w teście PassmarkCPU (wartość CPU Mark) zgodnie z wynikami opublikowanymi na stronie. [http://www.cpubenchmark.net/cpu\_list.php.](http://www.cpubenchmark.net/cpu_list.php)  Taktowanie bazowe minimum 2,00 GHz | |
| 1.1 | Opis sposobu weryfikacji wyników testu przedstawionego w ofercie wykonawcy | Wykonawca zobowiązany jest załączyć do oferty wydruk z ww. strony z wynikiem testu dla zaoferowanego procesora z datą nie wcześniejszą niż 7 dni przed upływem terminu składania ofert. | | |
| 2 | Pamięć RAM | Minimum 8 GB DDR 4 z możliwością rozbudowy do 32 GB | | |
| 3 | Dysk twardy | Minimum 250 GB SSD lub NVME M.2 | | |
| 4 | Karta graficzna | Zintegrowana z procesorem z dynamicznie przydzielaną pamięcią współdzieloną lub/i zewnętrzna karta graficzna z min. 2 GB pamięci własnej niewspółdzielonej, złącza karty graficznej HDMI lub DisplayPort | | |
| 5 | Obudowa | Suma wymiarów obudowy (wysokość + szerokość + głębokość) mierzona po krawędziach nie może przekraczać 700 mm, obudowa przystosowana **do pracy w poziomie.** | | |
| 6 | Złącza zewnętrzne | co najmniej 4 porty USB na tylnym panelu, w tym co najmniej 2 porty USB 3.0, minimum 2 porty USB, w tym minimum 1 USB 3.0 na panelu przednim. | | |
| 7 | Karta sieciowa | Ethernet 100/1000 Mbps, + Wi-Fi 6 (802.11a/b/g/n/ac/ax) | | |
| 8 | Karta dźwiękowa | Karta zintegrowana z płytą główną, gniazda słuchawek i mikrofonu wyprowadzone na przedni panel obudowy lub port combo | | |
| 9 | Zasilanie komputera | 230V ± 10%, 50 Hz, - sprawność zasilacza na poziomie 80% przy 20, 50 i 100 % obciążeniu. | | |
| 10 | Zainstalowane oprogramowanie systemowe | Zainstalowany Microsoft Windows 10 Pro PL 64-bit lub równoważny, o parametrach równoważności podanych poniżej. Zainstalowany system operacyjny nie wymagający już aktywacji za pomocą telefonu lub Internetu w firmie producenta oprogramowania. Parametry równoważności: Pełna integracja z domeną Active Directory MS Windows (posiadaną przez Zamawiającego) opartą na serwerach Windows Server 2012; Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), WMI; Pełna integracja Płatnik; Pełna obsługa ActiveX. Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji. | | |
| 11 | Klawiatura | Pełnowymiarowy, czytelny i kontrastowy układ w polskim standardzie QWERTY z wydzielonymi klawiszami nawigacyjnymi i klawiaturą numeryczną, przewodowa  - USB, długość przewodu minimum 1,8m | | |
| 12 | Urządzenie wskazujące | Mysz optyczna przewodowa – USB, min. 800DPI, długość przewodu minimum 1,8 m | | |
| 13 | Wsparcie techniczne | Dostęp do aktualnych sterowników zainstalowanych w komputerze urządzeń, realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego komputera, na dedykowanej przez producenta stronie internetowej – należy podać adres strony oraz sposób realizacji wymagania (opis uzyskania w/w informacji) | | |
| 14 | Wymagania dodatkowe | 1. Komputer musi być wyposażony w zabezpieczenie sprzętowe umożliwiające zabezpieczenie haseł użytkowników, administratora oraz danych użytkownika. Zabezpieczenie ma składać się z dedykowanego urządzenia szyfrującego (współpracującego z płytą główną), którego usunięcie uniemożliwi uruchomienie komputera, a odczyt zabezpieczonych danych z dysku twardego nie będzie możliwy na innym komputerze. | | |
| 15 | Niezawodność / jakość wytwarzania | Potwierdzona certyfikatami:  Certyfikat CE  ISO 14001  ISO 9001 | | |
| 16 | Gwarancja | Minimum 24 miesiące licząc od daty podpisania protokołu odbioru końcowego dostaw, wchodzących w zakres przedmiotu zamówienia, wykonanych bez zastrzeżeń. Gwarancja realizowana od daty wystawienia faktury. Usunięcie awarii – w ciągu 5 dni roboczych od otrzymania zgłoszenia (przyjmowanie zgłoszeń w dni robocze w godzinach 8.00-15.00 telefonicznie), w przypadku braku możliwości naprawy w w/w terminie podstawienie sprzętu zastępczego o nie gorszych parametrach technicznych.  Serwis urządzeń musi byś realizowany przez producenta lub autoryzowanego partnera serwisowego producenta . | | |

1. **Komputer przenośny - laptop konwertowalny 1 szt.**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Nazwa elementu, parametru lub cechy** | **Wymagania minimalne** |
|  | **Komputer przenośny - laptop konwertowalny** | |
| 1 | Wielkość matrycy (przekątna) | 14 cali |
| 2 | Wydajność procesora | Procesor wielordzeniowy, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej niż 10500 pkt. na podstawie MassMark PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na stronie http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego modelu procesora. |
| 3 | Ilość pamięci RAM | Minimum 16 GB DDR4 |
| 4 | Rodzaj dysku twardego | Półprzewodnikowy (SSD – solid-state drive) M.2 NVMe PCIe |
| 5 | Pojemność dysku twardego | Minimum 500 GB |
| 6 | Rodzaj matrycy | dotykowa |
| 7 | Rozdzielczość matrycy | co najmniej 1920 x 1080 pikseli |
| 8 | Rodzaj karty graficznej | zintegrowana |
| 9 | Łączność bezprzewodowa | Wi-Fi 6 (802.11ax) + Bluetooth 5.0 |
| 10 | Klawiatura | Podświetlona klawiatura odporna na zachlapanie cieczą |
| 11 | Kamera internetowa | 720p HD z wbudowaną przesłoną do ochrony prywatności |
| 12 | Wejścia/wyjścia | Minimum: 1 x USB 3.2; 2 x USB C ; 1 x HDMI; 1 x Ethernet RJ-45; 1 x audio typu combo (mini-jack 3,5 mm); 1 x czytnik kart microSD; wymagana ilość wszystkich portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. |
| 13 | Bateria i zasilanie | Bateria min. 50 Wh.  Zasilacz min. 65W. |
| 14 | Waga | maksymalnie 1650 gram |
| 15 | Możliwość pracy w trybie tabletu | przekształcenie w tablet poprzez obrót ekranu na zawiasach, w taki sposób, że tylna obudowa matrycy opiera się na dolnej obudowie korpusu laptopa. |
| 16 | Zabezpieczenia | Trusted Platform Module (TPM) 2.0, zintegrowany czytnik linii papilarnych. |
| 17 | System operacyjny | Zainstalowany Microsoft Windows 10 Pro PL 64-bit lub równoważny, o parametrach równoważności podanych poniżej. Zainstalowany system operacyjny nie wymagający już aktywacji za pomocą telefonu lub Internetu w firmie producenta oprogramowania. Parametry równoważności: Pełna integracja z domeną Active Directory MS Windows (posiadaną przez Zamawiającego) opartą na serwerach Windows Server 2012; Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), WMI; Pełna integracja Płatnik; Pełna obsługa ActiveX. Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji. |
| 18 | Dodatkowe akcesoria | Dedykowany rysik do ekranu, HUB USB-C – minimum 4 x USB, instrukcja obsługi. |
| 19 | Torba transportowa | Wyposażona w 3 komory zapinane zamkiem błyskawicznym z dwoma suwakami każdy. Wykonana z poliuretanów lub poliamidów. Dwie komory główne, z czego jedna dedykowana komora do transportu laptopa. Trzecia komora z kieszonkami na akcesoria takie jak telefon, długopisy, mysz bezprzewodowa. Torba wyposażona w uchwyt do noszenia w ręce oraz w regulowany, odpinany pasek do noszenia na ramieniu. |
| 20 | Certyfikaty i standardy | US MIL-STD 810H, EPEAT, Energy Star, CE |
| 21 | Gwarancja | Minimum 24 miesiące licząc od daty podpisania protokołu odbioru końcowego dostaw, wchodzących w zakres przedmiotu zamówienia, wykonanych bez zastrzeżeń. Gwarancja realizowana od daty wystawienia faktury. Usunięcie awarii – w ciągu 5 dni roboczych po otrzymaniu zgłoszenia (przyjmowanie zgłoszeń w dni robocze w godzinach 8.00-15.00 telefonicznie), w przypadku braku możliwości naprawy w w/w terminie podstawienie sprzętu zastępczego o nie gorszych parametrach technicznych. W przypadku awarii dysków twardych w okresie gwarancji, dyski pozostają u Zamawiającego.  Serwis urządzeń musi byś realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane oświadczenie Wykonawcy potwierdzające, że serwis będzie realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta. |

**CZĘŚĆ 2 – URZĄDZENIA UTM**

**Urządzenia UTM – 2 szt.**

**Wymagania Ogólne**

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

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

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

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

**Redundancja, monitoring i wykrywanie awarii**

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

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:

* 5 portami Gigabit Ethernet RJ-45.

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 100 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 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 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 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 także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

**Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.

**Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/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.
* Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

**Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

**Funkcje SD-WAN**

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

**Zarządzanie pasmem**

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

**Ochrona przed malware**

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

**Ochrona przed atakami**

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

**Kontrola aplikacji**

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

**Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja 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 url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

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

**Logowanie**

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

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

**Serwisy i licencje**

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

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 24 miesiące.

**Gwarancja oraz wsparcie**

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**Opisy do wymagań ogólnych**

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