Załącznik nr 2b do SWZ

**Aktualny Opis przedmiotu zamówienia dla części 2- po zmianie z dn. 23.06.2023 r.**

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | **Oferowane parametry, nazwa i model urządzenia lub nazwa oprogramowania lub świadczonej usługi**  **(Uwaga wypełniamy tylko białe pola!)** |
| Typ | Urządzenie zabezpieczające UTM z licencją- 1 sztuka | Producent:  Model:  Numer katalogowy (numer konfiguracji lub part numer): |
| Zastosowanie | Zabezpieczenie sieci komputerowej |  |
| Urządzenie | Urządzenie zabezpieczające ze specjalistycznym oprogramowaniem. Wykrywanie i zapobieganie zagrożeniom, funkcja firewall'a, zapobiegania włamaniom, ochrony antyspamowej czy filtrowania stron www. | Producent:  Nazwa:  Model: |
| Wsparcie | Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta | TAK/NIE\* |
| Obudowa | Obudowa dostarczona z kompletem mocowań do szafy RACK 19” | TAK/NIE\* |
| Wymagania 1 | Wymagane interfejsy:  Port USB (klient/serwer) - 1 Port konsoli RJ-45 - 1 Port GE RJ45 MGMT/DMZ -2 Port GE RJ45 WAN - 2 Port GE Rj45 HA - 2 Port GE RJ45 - 12 Port GE SFP - 4 Przepustowość Firewall (1518 byte UDP) - 20Gbps Przepustowość Firewall (512 byte UDP) - 18Gbps Przepustowość Firewall (64 byte UDP) - 10Gbps Przepustowość Firewall (PPS) –15 Mpps Ilość jednoczesnych sesji (TCP) –1500000 Ilość nowych sesji/sekundę (TCP) - 56000 Ilość polityk zapory - 10 000 Przepustowość IPSec VPN (512 bytepacket) –11,5Gbps Przepustowość IPS (HTTP/Enterprise) - 800 / 270 Mbps Ilość tuneli Gateway-to-Gateway IPSec VPN – 2500 Ilość tuneli Client-to-Gateway IPSec VPN - 16000 Min ilość użytkowników SSL-VPN – 60 Przepustowość SSL-VPN –1 Gbps Dostępność - Active/Active,Active/Passive, Clustering Pamięć wewnętrzna 480 GB SSD | TAK/NIE\* |
| Wymagania 2 | Musi posiadać ochronę przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS | TAK/NIE\* |
| Wymagania 3 | Możliwość analizy ruchu szyfrowanego SSL i SSH | TAK/NIE\* |
| Wymagania 4 | Oprogramowanie urządzenia musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą: - Haseł statycznych i definicji w lokalnej bazie systemu - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP - haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu SSO w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny | TAK/NIE\* |
| Wymagania 5 | Budowanie polityk w oparciu o adres IP, użytkownika, protokół, usługę sieciową, aplikację, reakcję zabezpieczeń z możliwością budowania zbiorów w oparciu o powyższe zmienne | TAK/NIE\* |
| Wymagania 6 | Ochrona przed atakami (IPS) musi: - opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. - uwzględniać aplikacje pracujące na niestandardowych portach - posiadać automatycznie aktualizowaną bazę zawierającą minimum 5000 sygnatór - umożliwiać tworzenie własnych sygnatur oraz wyjątków - zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS - zapewnić 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 - Wykrywać i blokować komunikację botnet | TAK/NIE\* |
| Wymagania 7 | Moduł kontroli stron WWW musi: - korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. - posiadać kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxyavoidance. - Mieć możliwość filtrowania kategorii stron zabronionych prawem: Hazard. - Udostępniać możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  - umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł kontroli stron WWW. | TAK/NIE\* |
| Gwarancja | 24 miesiące | TAK/NIE\* |

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | **Oferowane parametry, nazwa i model urządzenia lub nazwa oprogramowania lub świadczonej usługi**  **(Uwaga wypełniamy tylko białe pola!)** |
| Typ | Urządzenie zabezpieczające UTM Wifi z licencją- 1 sztuka | Producent:  Model:  Numer katalogowy (numer konfiguracji lub part numer): |
| Zastosowanie | Zabezpieczenie sieci komputerowej |  |
| Urządzenie | Urządzenie zabezpieczające ze specjalistycznym oprogramowaniem. Wykrywanie i zapobieganie zagrożeniom, funkcja firewall'a, zapobiegania włamaniom, ochrony antyspamowej czy filtrowania stron www. | Producent:  Nazwa:  Model: |
| Wsparcie | Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta | TAK/NIE\* |
| Obudowa | Obudowa dostarczona z kompletem mocowań do szafy RACK 19” | TAK/NIE\* |
| Wymagania 1 | Wymagane interfejsy:  Port USB (klient/serwer) - 1 Port konsoli RJ-45 - 1 Port GE RJ45DMZ - 1 Port GE RJ45 WAN - 2 Port GE RJ45 - 5 Przepustowość Firewall (1518 byte UDP) - 10Gbps Przepustowość Firewall (512 byte UDP) - 10Gbps Przepustowość Firewall (64 byte UDP) - 6Gbps Przepustowość Firewall (PPS) – 9Mpps Ilość jednoczesnych sesji (TCP) – 700000 Ilość nowych sesji/sekundę (TCP) - 35000 Ilość polityk zapory -  5000 Przepustowość IPSec VPN (512 bytepacket) – 6,5 Gbps Przepustowość IPS HTTPS - 630Mbps Ilość tuneli Gateway-to-Gateway IPSec VPN – 200 Ilość tuneli Client-to-Gateway IPSec VPN - 500 Min ilość użytkowników SSL-VPN – 60 Przepustowość SSL-VPN – 900Mbps Dostępność - Active/Active,Active/Passive, Clustering Pamięć wewnętrzna 128 GB SSD | TAK/NIE\* |
| Wymagania 2 | Musi posiadać ochronę przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS | TAK/NIE\* |
| Wymagania 3 | Możliwość analizy ruchu szyfrowanego SSL i SSH | TAK/NIE\* |
| Wymagania 4 | Oprogramowanie urządzenia musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą: - Haseł statycznych i definicji w lokalnej bazie systemu - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP - haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu SSO w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny | TAK/NIE\* |
| Wymagania 5 | Budowanie polityk w oparciu o adres IP, użytkownika, protokół, usługę sieciową, aplikację, reakcję zabezpieczeń z możliwością budowania zbiorów w oparciu o powyższe zmienne | TAK/NIE\* |
| Wymagania 6 | Ochrona przed atakami (IPS) musi: - opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. - uwzględniać aplikacje pracujące na niestandardowych portach - posiadać automatycznie aktualizowaną bazę zawierającą minimum 5000 sygnatór - umożliwiać tworzenie własnych sygnatur oraz wyjątków - zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS - zapewnić 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 - Wykrywać i blokować komunikację botnet | TAK/NIE\* |
| Wymagania 7 | Moduł kontroli stron WWW musi: - korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. - posiadać kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxyavoidance. - Mieć możliwość filtrowania kategorii stron zabronionych prawem: Hazard. - Udostępniać możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  - umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł kontroli stron WWW. | TAK/NIE\* |
| Gwarancja | 24 miesiące | TAK/NIE\* |

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | **Oferowane parametry, nazwa i model urządzenia lub nazwa oprogramowania lub świadczonej usługi**  **(Uwaga wypełniamy tylko białe pola!)** |
| Typ | Urządzenie zabezpieczające pocztę mailową z licencją- 1 sztuka | Producent:  Model:  Numer katalogowy (numer konfiguracji lub part numer): |
| Zastosowanie | Zabezpieczenie poczty mailowej |  |
| Urządzenie | Urządzenie do skanowania poczty elektronicznej zapewniające ochronę sieci przed spamem, szkodliwym oprogramowaniem oraz zagrożeniami rozprzestrzeniającymi się za pomocą poczty elektronicznej. | Producent:  Nazwa:  Model: |
| Wsparcie | Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta | TAK/NIE\* |
| Obudowa | Obudowa dostarczona z kompletem mocowań do szafy RACK 19” | TAK/NIE\* |
| Wymagania | - Port GE RJ45: 4 - Pojemność pamięci: 1TB - Liczba obsługiwanych domen: 20 - Skrzynki pocztowe w trybie serwera: 150 - Routing wiadomości e-mail: 50000 wiadomości/godz - Antyspami + Antywirus 40000 wiadomości/godz. | TAK/NIE\* |
| Gwarancja | 24 miesiące | TAK/NIE\* |

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | **Oferowane parametry, nazwa i model urządzenia lub nazwa oprogramowania lub świadczonej usługi**  **(Uwaga wypełniamy tylko białe pola!)** |
| Typ | Przełącznik Sieciowy (rozdzielacz) - 3 sztuki | Producent:  Model: |
| Zastosowanie | Przełącznik Sieciowy |  |
| Obudowa | Obudowa dostarczona z kompletem mocowań do szafy RACK 19” | TAK/NIE\* |
| Zarządzanie | - interfejs graficzny (WWW) - SSH (CLI) | TAK/NIE\* |
| Wymagania dodatkowe: | - Port Base-T: 24 x 1Gb/s - Port SFP+: 2 x 10Gb/s - Warstwa: L2 - Przepustowość: 96Mbps - Rozmiar tablicy MAC: 16000 - Ilość VLAN: 512 | TAK/NIE\* |
| Gwarancja | 24 miesiące | TAK/NIE\* |

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | **Oferowane parametry, nazwa i model urządzenia lub nazwa oprogramowania lub świadczonej usługi**  **(Uwaga wypełniamy tylko białe pola!)** |
| Typ | Przełącznik Sieciowy- 4 sztuki | Producent:  Model: |
| Zastosowanie | Przełącznik Sieciowy |  |
| Zarządzanie | - przeglądarka (WWW) | TAK/NIE\* |
| Wymagania dodatkowe: | - 8 x RJ 45 10/100/1000 Mbps - Warstwa: L2 - Przepustowość: 16 Gb/s | TAK/NIE\* |
| Gwarancja | 24 miesiące | TAK/NIE\* |

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | **Oferowane parametry, nazwa i model urządzenia lub nazwa oprogramowania lub świadczonej usługi**  **(Uwaga wypełniamy tylko białe pola!)** |
| Typ | Usługi informatyczne w zakresie wdrożenia sprzętu informatycznego oraz oprogramowania dotyczącego urządzenia zabezpieczającego UTM | TAK/NIE\* |
| Wymagania | Przygotowanie urządzenia do pracy w urzędzie, tj. rozpakowanie, ustawienie, podłączenie, konfiguracja. | TAK/NIE\* |

|  |  |  |
| --- | --- | --- |
| Nazwa komponentu | Wymagane minimalne parametry techniczne | **Oferowane parametry, nazwa i model urządzenia lub nazwa oprogramowania lub świadczonej usługi**  **(Uwaga wypełniamy tylko białe pola!)** |
| Typ | Usługi informatyczne w zakresie wdrożenia sprzętu informatycznego oraz oprogramowania dotyczącego urządzenia zabezpieczającego UTM WiFi | TAK/NIE\* |
| Wymagania | Przygotowanie urządzenia do pracy w urzędzie, tj. rozpakowanie, ustawienie, podłączenie, konfiguracja. | TAK/NIE\* |

\* Niepotrzebne skreślić