**1. URZĄDZENIA NGFW TYPU A - 1 KOMPLET (2 SZTUKI), URZĄDZENIA PRACUJĄCE W KLASTRZE NIEZAWODNOŚCIOWYM W PLACÓWCE SZPITALNEJ W LOKALIZACJI W GDYNI**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Podzespół** | **Należy wypełnić zgodnie z instrukcją zawartą w poszczególnych komórkach niniejszej kolumny** |
| **-1-** | **-2-** | **-3-** |
| 1 | Urządzenie | Należy wpisać nazwę producenta, model oraz rok produkcji oferowanego urządzenia:Producent Model Rok produkcji  |
| 2 | Parametry wydajnościowe | Należy wpisać: a. przepustowości firewall/kontroli aplikacji: b. przepustowości firewall/kontroli aplikacji/IPS/Antywirus/Antymalware: c. przepustowość dla IPsec VPN: d. jednoczesnych sesji: e. nowych połączeń na sekundę: f. tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN: g. wirtualnych routerów posiadających odrębne tabele routingu: h. stref bezpieczeństwa: i. pojemność lokalnej pamięci dla systemu operacyjnego oraz dzienniki zdarzeń (logi):  |
| 3 | Parametry funkcjonalne | Należy wpisać:a. wysokość urządzenia (wyrażona w U) w szafie RACK 19”: b. ilość redundantnych zasilaczy AC 230V Hot-Swap z kompletami kabli: c. ilość portów 10-GigabitEthernet RJ45: d. ilość portów 10 GigabitEthernet SFP+ obsługujących moduły optyczne SR oraz LR: e. ilość portów 25 GigabitEthernet SFP28: f. ilość portów 1 GigabitEthernet RJ45 lub 10 GigabitEthernet RJ45 wyłącznie do celów zarządzania: g. ilość dedykowanych/wydzielonych portów 2,5G lub 5G lub 10 GigabitEthernet lub szybszy dla celów połączenia urządzeń w klaster (high availability):  |
| 4 | Cechy urządzenia | Należy wpisać (TAK/NIE):a. Rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM): b. Transparentne ustalenie tożsamości użytkowników: c. Realizowanie funkcjonalności Intrusion Prevention System (IPS): d. Realizowanie funkcjonalności Antywirus (AV): e. Realizowanie funkcjonalności Anty-Spyware / Anty-Malware: f. Realizowanie funkcjonalności kategoryzacji URL i filtracji URL: g. Realizowanie funkcjonalności ochrony DNS: h. Realizowanie funkcjonalności sandbox lokalny lub chmurowy tego samego producenta: i. Możliwość łączenia w klaster z zapewnieniem funkcji synchronizacji sesji w trybach Active-Active lub Active-Passive: j. Blokowanie transmisji plików (co najmniej: bat, cab, pliki MS Office w tym zawierających makra, rar, zip, exe, gzip, hta, pdf, tar, tif) z rozpoznawaniem pliku na podstawie nagłówka i typu MIME: k. Filtrowanie ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron: l. Ochrona przed zagrożeniami Zero Day oraz zapewnienie współpracy z sandboxem: m. Ochrona DNS: n. Deszyfracja wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS: o. Obsługa połączeń VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site: p. Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN: r. Obsługa protokołów routingu OSPFv2 i OSPFv3, BGP4: s. Obsługa 4094 VLAN zgodnych z 802.1q: t. Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3: u. Obsługa własnych stref bezpieczeństwa: w. Translacja statyczna i dynamiczna adresów IP (NAT): x. Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego: y. Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH:  |
| 5 | Wyposażenie dodatkowe | Należy wpisać (TAK/NIE):a. Komplet dokumentacji dla użytkownika w formie papierowej/elektronicznej w języku polskim lub angielskim (wersja angielska dopuszczalna w przypadku braku dostępności wersji polskiej dokumentacji): b. Niezbędne wyposażenie (przewody zasilające, sygnałowe, szyny i elementy montażowe itp.):  |
| 6 | Licencje i subskrypcje (60 miesięcy) | Należy wpisać rodzaj dostarczonych licencji i subskrypcji:      |
| 7 | Zaawansowana ochrona DNS w trybie rzeczywistym | Należy wpisać TAK lub NIE i wskazać dostarczony dokument techniczny producenta oferowanego urządzenia (z podaniem stron) z opisem spełnienia wymaganych w SWZ zapisów **(parametr dodatkowo punktowany):**      |
| 8 | Ochrona z wykorzystaniem mechanizmów machine learning | Należy wpisać TAK lub NIE i wskazać dostarczony dokument techniczny producenta oferowanego urządzenia (z podaniem stron) z opisem spełnienia wymaganych W SWZ zapisów **(parametr dodatkowo punktowany):**      |
| 9 | Możliwość wykorzystania posiadanych rozwiązań bezpieczeństwa | Należy wpisać TAK lub NIE i wskazać dostarczony dokument techniczny producenta oferowanego urządzenia (z podaniem stron) z opisem spełnienia wymaganych w SWZ zapisów **(parametr dodatkowo punktowany):**      |
| 10 | Realizacja zdalnego dostępu bez konieczności migracji oprogramowania klienta vpn Zamawiającego | Należy wpisać TAK lub NIE i wskazać dostarczony dokument techniczny producenta oferowanego urządzenia (z podaniem stron) z opisem spełnienia wymaganych SWZ zapisów **(parametr dodatkowo punktowany):**      |

**2. URZĄDZENIA NGFW TYPU B – 2 KOMPLETY (4 SZTUKI), URZĄDZENIA PRACUJĄCE W KLASTRZE NIEZAWODNOŚCIOWYM DLA PLACÓWEK SZPITALNYCH W LOKALIZACJI: W GDYNI ORAZ W WEJHEROWIE**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Podzespół** | **Należy wypełnić zgodnie z instrukcją zawartą w poszczególnych komórkach niniejszej kolumny** |
| **-1-** | **-2-** | **-3-** |
| 1 | Urządzenie | Należy wpisać nazwę producenta, model oraz rok produkcji oferowanego urządzenia:Producent Model Rok produkcji  |
| 2 | Parametry wydajnościowe | Należy wpisać: a. przepustowości firewall/kontroli aplikacji: b. przepustowości firewall/kontroli aplikacji/IPS/Antywirus/Antymalware: c. przepustowość dla IPsec VPN: d. jednoczesnych sesji: e. nowych połączeń na sekundę: f. tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN: g. wirtualnych routerów posiadających odrębne tabele routingu: h. stref bezpieczeństwa: i. pojemność lokalnej pamięci dla systemu operacyjnego oraz dzienniki zdarzeń (logi):  |
| 3 | Parametry funkcjonalne | Należy wpisać:a. wysokość urządzenia (wyrażona w U) w szafie RACK 19”: b. ilość redundantnych zasilaczy AC 230V Hot-Swap z kompletami kabli: c. ilość portów 10-GigabitEthernet RJ45: d. ilość portów 10 GigabitEthernet SFP+ obsługujących moduły optyczne SR oraz LR: e. ilość portów 25 GigabitEthernet SFP28: f. ilość portów 1 GigabitEthernet RJ45 lub 10 GigabitEthernet RJ45 wyłącznie do celów zarządzania: g. ilość dedykowanych/wydzielonych portów 2,5G lub 5G lub 10 GigabitEthernet lub szybszy dla celów połączenia urządzeń w klaster (high availability):  |
| 4 | Cechy urządzenia | Należy wpisać (TAK/NIE):a. Rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM): b. Transparentne ustalenie tożsamości użytkowników: c. Realizowanie funkcjonalności Intrusion Prevention System (IPS): d. Realizowanie funkcjonalności Antywirus (AV): e. Realizowanie funkcjonalności Anty-Spyware / Anty-Malware: f. Realizowanie funkcjonalności kategoryzacji URL i filtracji URL: g. Realizowanie funkcjonalności ochrony DNS: h. Realizowanie funkcjonalności sandbox lokalny lub chmurowy tego samego producenta: i. Możliwość łączenia w klaster z zapewnieniem funkcji synchronizacji sesji w trybach Active-Active lub Active-Passive: j. Blokowanie transmisji plików (co najmniej: bat, cab, pliki MS Office w tym zawierających makra, rar, zip, exe, gzip, hta, pdf, tar, tif) z rozpoznawaniem pliku na podstawie nagłówka i typu MIME: k. Filtrowanie ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron: l. Ochrona przed zagrożeniami Zero Day oraz zapewnienie współpracy z sandboxem: m. Ochrona DNS: n. Deszyfracja wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS: o. Obsługa połączeń VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site: p. Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN: r. Obsługa protokołów routingu OSPFv2 i OSPFv3, BGP4: s. Obsługa 4094 VLAN zgodnych z 802.1q: t. Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3: u. Obsługa własnych stref bezpieczeństwa: w. Translacja statyczna i dynamiczna adresów IP (NAT): x. Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego: y. Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH:  |
| 5 | Wyposażenie dodatkowe | Należy wpisać (TAK/NIE):a. Komplet dokumentacji dla użytkownika w formie papierowej/elektronicznej w języku polskim lub angielskim (wersja angielska dopuszczalna w przypadku braku dostępności wersji polskiej dokumentacji): b. Niezbędne wyposażenie (przewody zasilające, sygnałowe, szyny i elementy montażowe itp.):  |
| 6 | Licencje i subskrypcje (60 miesięcy) | Należy wpisać rodzaj dostarczonych licencji i subskrypcji:      |
| 7 | Zaawansowana ochrona DNS w trybie rzeczywistym | Należy wpisać TAK lub NIE i wskazać dostarczony dokument techniczny producenta oferowanego urządzenia (z podaniem stron) z opisem spełnienia wymaganych w SWZ zapisów **(parametr dodatkowo punktowany):**      |
| 8 | Ochrona z wykorzystaniem mechanizmów machine learning | Należy wpisać TAK lub NIE i wskazać dostarczony dokument techniczny producenta oferowanego urządzenia (z podaniem stron) z opisem spełnienia wymaganych w SWZ zapisów **(parametr dodatkowo punktowany):**      |
| 9 | Możliwość wykorzystania posiadanych rozwiązań bezpieczeństwa | Należy wpisać TAK lub NIE i wskazać dostarczony dokument techniczny producenta oferowanego urządzenia (z podaniem stron) z opisem spełnienia wymaganych w SWZ zapisów **(parametr dodatkowo punktowany):**      |
| 10 | Realizacja zdalnego dostępu bez konieczności migracji oprogramowania klienta vpn Zamawiającego | Należy wpisać TAK lub NIE i wskazać dostarczony dokument techniczny producenta oferowanego urządzenia (z podaniem stron) z opisem spełnienia wymaganych w SWZ zapisów **(parametr dodatkowo punktowany):**      |

**3. SERWEROWE DYSKI TWARDE DO ROZBUDOWY SERWERA SYSTEMOWEGO ZARZĄDZANIA CENTRALNEGO (SZC) PALO ALTO PANORAMA VM (będącego na wyposażeniu Zamawiającego) – 4 SZTUKI**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Podzespół** | **Należy wypełnić zgodnie z instrukcją zawartą w poszczególnych komórkach niniejszej kolumny** |
| **-1-** | **-2-** | **-3-** |
| 1 | Urządzenie | Należy wpisać nazwę producenta, model oraz rok produkcji oferowanego urządzenia:Producent Model Rok produkcji  |
| 2 | Parametry | Należy wpisać: Rozmiar kieszeni dysku SSD: Pojemność pamięci SSD: Standardowe rozwiązania komunikacyjne: Typ pamięci: Szybkość przesyłania danych: Gbit/sPrędkość odczytu z nośnika: MB/sPrędkość zapisu nośnika: MB/sLosowy odczyt (4KB): IOPSLosowy zapis (4KB): IOPSOpóźnienie odczytu: µsOpóźnienie zapisu: µs |

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

Kwalifikowany podpis elektroniczny osoby upoważnionej do reprezentowania Wykonawcy