Przedmiot zamówienia: **Dostawa urządzeń transmisji danych: firewall-e**

**Arkusz cenowy**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Cena brutto razem (w zł)** |
| *1* | *2* | *3* |
| 1. | Łączna cena (brutto) za Firewall rdzeniowy przedstawiony w Tabeli 1 niniejszego załącznika |  |
| 2. | Łączna cena (brutto) za Firewall internetowy z zaawansowanymi mechanizmami filtracji UTM przedstawiony w Tabeli 2 niniejszego załącznika |  |
| **Cena brutto oferty (poz. 1+2):** | |  |

Spis tabel

[**Tabela 1.** **Firewall rdzeniowy** 3](#_Toc12869558)

[**Tabela 2.** **Firewall internetowy z zaawansowanymi mechanizmami filtracji UTM** 12](#_Toc12869559)

# **Firewall rdzeniowy**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Przedmiot** | | **Cena jednostkowa netto [zł]** | **Kwota jednostkowa VAT (23%) [zł]** | **Cena jednostkowa brutto [zł]** | **Ilość**  **[szt.]** | **Cena całkowita brutto [zł]** | **Producent, model oraz parametry**  **(w tabeli uzupełnić tylko miejsca wykropkowane)** |
| *1* | | *2* | *3* | *4=2+3* | *5* | *6=4x5* | *7* |
| **Firewall rdzeniowy** | | …………….. | ………. | …………... | 2 | ………………… | **Producent………………………………….…….**  **Model…………………………………………….** |
| **Lp.** | **Parametr wymagany** | | | | | |  |
| 1 | Montaż w szafach Rack 19” posiadanych przez Zamawiającego. Wykonawca dostarczy komplet elementów montażowych w szczególności szyny montażowe. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 2 | Rozmiar urządzenia nie więcej niż 2U | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 3 | Co najmniej dwa redundantnie pracujące zasilacze 230V. Awaria jednego zasilacza nie wpływa na pracę oraz wydajność urządzenia. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 4 | Dostarczony komplet kabli zasilających umożliwiający podłączenie wszystkich zasilaczy do gniazd IEC320 C13 | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 5 | Urządzenie umożliwiające routing IPv4 oraz IPv6 z możliwością filtracji ruchu | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 6 | Interfejsy o sumarycznej przepustowości mnie mniejszej niż 80Gbps w konfiguracji 8x SFP+ 10Gbps lub 2xQSFP+ 40Gbps  Dodatkowo co najmniej  16 interfejsów 1Gbps SFP 16 interfejsów 1Gbps RJ45 | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 7 | Podłączenie dostarczanego sprzętu do Infrastruktury Zamawiającego. W szczególności do przełączników HPE FlexNetwork (Comware) posiadanych przez Zamawiającego. Do podłączenia po stronie sprzętu obecnie posiadanego przez Zamawiającego należy wykorzystać 8 portów SFP+ w czterech przełącznikach HPE 5700 (4x2) lub 2 porty QSFP+ w dwóch przełącznikach HPE 10500 (2x1). Dopuszcza się wykorzystanie rozszytego połączenia QSFP+ 40Gbps na przełączniku HPE 10500 na 4 niezależne interfejsy 10Gbps. Wolne porty SFP+ lub QSFP+ udostępnia Zamawiający.  Wszystkie pozostałe elementy podłączenia w szczególności moduły SFP+ lub QSFP+, kable przyłączeniowe stanowią element dostawy. Wkładki lub kable DAC SFP+ lub QSFP+ powinny pochodzić z oficjalnych kanałów sprzedaży producenta przełączników i firewalla. Nie dopuszcza się stosowania tzw. zamienników, które nie będą niewspierane przez dostawców urządzeń. Urządzenia zostaną zamontowane w pomieszczeniach serwerowych Zamawiającego w Krakowie przy ul. Jakubowskiego 2 w budynku G i H. Wykonawca pokrywa całość kosztów połączenia, w szczególności wykonania niezbędnych połączeń światłowodowych pomiędzy serwerowniami w budynkach G i H. Ilość połączeń powinna być wystarczająca do uruchomienia dostarczonego sprzętu ale nie mniej niż 48 włókien światłowodowych OM4 zakończonych na panelu krosowym ze złączami MPO. Jakość wykonania tras światłowodowych powinny zostać zmierzona raport pomiarowy dostarczony Zamawiającemu. | | | | | | **Parametr punktowany**  **Wykorzystanie do połącznia interfejsów QSFP+ w przełącznikach HPE 10500**  **TAK - 10 punków**  **NIE – 0 punktów**  **………………..**  *(podać TAK/NIE)* |
| 8 | Obsługa połączeń agregowanych typu LACP trunk w szczególności możliwość utworzenia połączenia zbiorczego dla interfejsów 10Gbps/40Gbps o przepustowości maksymalnej nie mniejszej 80Gbps. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 9 | Urządzenie musi umożliwiać tworzenie interfejsów VLAN 802.1Q zarówno dla interfejsów fizycznych oraz agregowanych (w szczególności dla połączenia opisanego w poprzednim punkcie) | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 10 | Urządzenie musi umożliwiać tworzenie interfejsów typu bridge funkcjonujących na zasadzie przełącznika Ethernet. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 11 | Całkowita ilość obsługiwanych interfejsów fizycznych oraz logicznych (VLAN) nie mniejsza niż 4000 | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 12 | Urządzenie musi umożliwiać uruchomienie co najmniej 400 serwerów DHCP na interfejsach fizycznych oraz logicznych (VLAN). Możliwość zdefiniowania rezerwacji adresu IP po adresie MAC dla co najmniej 4000 adresów IP (łącznie). | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 13 | Obsługa DHCP Relay na co najmniej 400 interfejsach fizycznych oraz logicznych (VLAN). W ramach jednego interfejsu musi istnieć możliwość przekazania zapytań DHCP do co najmniej dwóch serwerów DHCP pracujących w trybie wysokiej dostępności. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 14 | Obsługa co najmniej 16000 adresów MAC w ramach protokołu ARP | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 15 | System powinien umożliwiać pracę jako serwer VPN dla połączeń site-to-site dla co najmniej 300 równoczesnych połączeń. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 16 | Dla VPN typu IPSec wsparcie dla protokołu IKE v1 oraz v2 oraz mechanizmów IPSec NAT Traversal, DPD, Xauth | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 17 | Wydajność IPSec VPN nie mniej niż 40Gbps | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 18 | System powinien umożliwiać pracę jako serwer VPN dla połączeń client-to-site dla co najmniej 1000 równoczesnych połączeń użytkowników. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 19 | W połaczeniach client-to-site obsługa split tunneligu (wyznaczenie określonych sieci tunelowania). | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 20 | Dedykowany klient vpn dla systemów Windows, Linux, OSX, Adnroid, iOS. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 21 | Dedykowany klient vpn dla systemu Windows powinien posiadać ochronę antywirusową uniemożliwiającą połączenie zawirusowanych systemów. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 22 | Logowania do vpn typu Client-To-Site przy pomocy loginu i hasła, certyfikatów PKI. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 23 | Możliwość uruchomienia w przyszłości funkcji dwuskładnikowego uwierzytelniania do VPN w formie aplikacji mobilnej na systemy Android/iOS oraz w formie fizycznego tokenu. Funkcja dwuskładnikowego uwierzytelniania powinna być możliwa do zrealizowania przez dostarczone urządzenie bez konieczności instalacji dodatkowej infrastruktury serwerowej. Funkcja dwuskładnikowego dla aplikacji mobilnej dostępna również w technologii push, opartej o komunikat potwierdzenia bez konieczności przepisywania kodów uwierzytelniających. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 24 | Dostęp do zasobów chronionych VPN w formie portalu obsługiwanego w całości przez przeglądarkę www w oparciu o HTML 5. Obsługa co najmniej HTTP, HTTPS, SMB/CIFS, SSH, RDP, VNC, FTP. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 25 | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 26 | Obsługa protokołów routingu RIP, OSPF, BGP | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 27 | Definiowanie routingu na pomocą polis, w szczególności na podstawie źródłowego adresu IP (PBR) | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 28 | Obsługa translacji adresów sieciowych NAT | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 29 | Maksymalna wydajność filtracji firewalla nie mniejsza niż 80Gbps oraz 80Mpps.  \* [Uwaga] Oceniana będzie maksymalna wydajność filtracji firewalla w przedziale od 80Gbps do 160Gbps. Jeżeli wykonawca zaoferuje wydajność filtracji firewalla większą niż 160 Gbps to Zamawiający i tak przyjmie do porównania ofert 160 Gbps. | | | | | | **Parametr punktowany**  **…………………. Gbps**  *(podać maks. przepustowość nie mniej niż* 80Gbps*)*  Liczba punktów Ff = (Ffi/Ffmax) \* 10  gdzie:  Ffi – maksymalna wydajność filtracji firewalla w ofercie ocenianej (min. 80Gbps),  Ffmax – największa wydajność filtracji firewalla spośród wszystkich ofert ocenianych (przy czym maksymalna wartość Ffmax to 160 Gbps). |
| 30 | Ilość równocześnie obsługiwanych sesji TCP nie mniejsza niż 10 milionów | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 31 | Urządzenie w politykach filtrowania musi obsługiwać tzw. zdefiniowane adresy w formach: adres CIDR (IP/maska), zakres adresów IP, nazwa FQDN. Minimalna liczba obsługiwanych zdefiniowanych adresów nie mniejsza niż 20000 | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 32 | Urządzenie w politykach filtrowania musi obsługiwać grupy adresów zdefiniowanych. Grupy powinny obejmować zbiory adresów zdefiniowanych oraz inne grupy. Maksymalna liczba członków grupy nie może być niższa niż 1500. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 33 | Mechanizm umożliwiający integrację z systemem Active Directory posiadanym przez Zamawiającego pozwalającym na ustaleniu adresów IP użytkowników zalogowanych do komputerów z sieci lokalnej i możliwości wykorzystania nazwy użytkownika w politykach filtrowania. Urządzenie musi także umożliwiać wykorzystanie grup użytkowników Active Directory. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 34 | Definiowanie polityk filtrowania ruchu w oparciu o: - strefy (zbiory interfejsów) - interfejs źródłowy - interfejs docelowy - źródłowy IP z możliwością wykorzystania zdefiniowanych adresów oraz użytkowników oraz grup użytkowników z Active Directory - docelowy IP - harmonogram czasowy - protokół (TCP/UDP) i numery portów | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 35 | Wydajność firewall’a dla rzeczywistego ruchu nie powinna być niższa niż 38000Mbps.  **Wyniki powinny opisywać metodę uzyskania pomiaru wydajności i być opublikowane przez niezależną od producenta organizację zajmującej się testowanie wydajności urządzeń sieciowych (np. NSSLABS). Zamawiający dopuszcza możliwość dostarczenia dokumentu dla urządzenia zbliżonego do oferowanego a różniącego się parametrami niemającymi wpływ na wydajność, np. inny rodzaj zasilania, inna konfiguracja interfejsów fizycznych.**  Zamawiający zastrzega sobie możliwość aby Wykonawca udowodnił osiągane parametry poprzez zestawienie środowiska testowego dla dostarczanego sprzętu i wygenerowaniu rzeczywistego ruchu o maksymalnej przepustowości. Jako ruch rzeczywisty przyjmując ciąg transakcji HTTP GET z odpowiedziami w rozmiarze 21KB lub inny uzgodniony z Zamawiającym. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 36 | Zarządzanie urządzeniem poprzez konsolę graficzną oraz interfejs tekstowy (cli) | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 37 | Urządzenie musi umożliwiać detekcję aplikacji wykorzystywanych w transmisji sieciowej z możliwością wykorzystania tej informacji przy politykach filtrowania ruchu. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 38 | Urządzenie umożliwia deszyfrację wybranego ruchu SSL | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 39 | Monitoring (mirror) wybranego ruchu sieciowego na dedykowanym porcie | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 40 | Urządzenie można rozbudować o mechanizmy IPS, Antywirusa i Filtrowania adresów URL bez konieczności dodawania dodatkowych elementów sprzętowych. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 41 | Wydajność mechanizmu IPS z uruchomioną kontrolą aplikacji po rozbudowie nie może być niższa niż 10Gbit/s dla realnego ruchu. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 42 | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikacje dla funkcjonalności firewall, IPS/NGFW i SSL VPN wystawiona przez niezależną organizację certyfikującą. Organizacja powinna mieć przeprowadzone certyfikacje dla co najmniej 5 różnych producentów urządzeń typu firewall dostępnych na rynku Polskim.  Przykładowo   * ICSA dla funkcji Firewall. * ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW. * ICSA dla funkcji SSL VPN. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 43 | Urządzenie wyposażone w pamięć stałą o pojemności co najmniej 200GB pozwalające na przechowywanie logów lub przechwycony ruch (packet capture). Urządzeni powinno być odporne na awarię jednego nośnika danych. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 44 | Wykonawca zamontuje oraz wstępnie skonfiguruje urządzenie zgodnie z ustaleniami z Zamawiającym. Dostarczone urządzenia powinny zostać skonfigurowane do pracy w trybie wysokiej dostępności. Awaria lub wyłączenie jednego urządzenia nie powoduje przestoju w pracy sieci komputerowej. Dodatkowo Wykonawca dokona migracji konfiguracji z zachowaniem wszystkich funkcjonalności z urządzenia Fortigate FG-600D obecnie używanego przez Zamawiającego oraz przełączy urządzenie obecnie używane na dostarczone. Czas przestoju pracy sieci komputerowej podczas przełączenia nie może byś dłuższy niż 2h. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 45 | Wyznaczonych trzech pracowników zostanie przeszkolonych z obsługi urządzenia w ramach autoryzowanego szkolenia producenta. Szkolenie powinno odbywać się w języku polskim w miejscowości Zamawiającego i trwać nie krócej niż 3 dni. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 46 | Gwarancja oraz Wsparcie techniczne dla produktu co najmniej 36 miesięcy. Serwis dostępny w trybie 24x7 przez 365 dni w roku. Wymiana uszkodzonego sprzętu w siedzibie zamawiającego najpóźniej następnego dnia roboczego. W cenie dostawy przedmiotu umowy dostęp do aktualizacji oprogramowania systemowego w trakcie trwania kontraktu serwisowego. Wsparcie techniczne dla firewalli rdzeniowych oraz firewalli internetowych muszą być realizowane przez jeden podmiot.  \* [Uwaga] Oceniana będzie całkowita liczba miesięcy w przedziale od 37 miesięcy do 72 miesięcy. Jeżeli wykonawca zaoferuje okres gwarancji i wsparcia technicznego dłuższy niż 72 miesiące, to Zamawiający i tak przyjmie do porównania ofert okres 72 miesięcy. | | | | | | **Parametr oceniany**  **Podać okres trwania gwarancji i wsparcia technicznego**  **………………………………..miesięcy**  **(podać okres w pełnych miesiącach na jaki zostanie udzielona gwarancja i wsparcie techniczne – min. 36 miesięcy)**  Liczba punktów Gw = (Gwi/Gwmax) \* 20  gdzie:  Gwi – liczba miesięcy gwarancji i wsparcia technicznego w ofercie ocenianej (min. 37 miesięcy),  Gwmax – największa liczba miesięcy gwarancji i wsparcia technicznego spośród wszystkich ofert ocenianych (przy czym maksymalna wartość Gwmax to 72 miesięcy). |

# **Firewall internetowy z zaawansowanymi mechanizmami filtracji UTM**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Przedmiot** | | **Cena jednostkowa netto [zł]** | **Kwota jednostkowa VAT (23%) [zł]** | **Cena jednostkowa brutto [zł]** | **Ilość**  **[szt.]** | **Cena całkowita brutto [zł]** | **Producent, model oraz parametry**  **(w tabeli uzupełnić tylko miejsca wykropkowane)** |
| *1* | | *2* | *3* | *4=2+3* | *5* | *6=4x5* | *7* |
| **Firewall internetowy z zaawansowanymi mechanizmami filtracji UTM** | | …………….. | ………. | …………... | 2 | ………………… | **Producent………………………………….…….**  **Model…………………………………………….** |
| **Lp.** | **Parametr wymagany** | | | | | |  |
| 1 | Montaż w szafach Rack 19” posiadanych przez Zamawiającego. Wykonawca dostarczy komplet elementów montażowych w szczególności szyny montażowe. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 2 | Rozmiar urządzenia nie więcej niż 2U. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 3 | Co najmniej dwa redundantnie pracujące zasilacze 230V. Awaria jednego zasilacza nie wpływa na pracę oraz wydajność urządzenia. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 4 | Dostarczony komplet kabli zasilających umożliwiający podłączenie wszystkich zasilaczy do gniazd IEC320 C13. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 5 | Urządzenie umożliwiające routing IPv4 oraz IPv6 z możliwością filtracji ruchu. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 6 | Interfejsy:  - co najmniej 2 interfejsy 10Gbps SFP+ - co najmniej 8 interfejsów 1Gbps SFP - co najmniej 8 interfejsów 1Gbps RJ45 | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 7 | Podłączenie dostarczanego sprzętu do Infrastruktury Zamawiającego w szczególności do firewallów rdzeniowych. powinny pochodzić z oficjalnych kanałów sprzedaży producenta przełączników i firewalla. Nie dopuszcza się stosowania tzw. zamienników. Urządzenia zostaną zamontowane w pomieszczeniach serwerowych Zamawiającego w Krakwie, przy ul. Jakubowskiego 2 w budynku G i H. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 8 | Obsługa połączeń agregowanych typu LACP trunk. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 9 | Urządzenie musi umożliwiać tworzenie interfejsów VLAN 802.1Q zarówno dla interfejsów fizycznych oraz agregowanych (w szczególności dla połączenia opisanego w poprzednim punkcie). | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 10 | Urządzenie musi umożliwiać tworzenie interfejsów typu bridge funkcjonujących na zasadzie przełącznika Ethernet. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 11 | Całkowita ilość obsługiwanych interfejsów fizycznych oraz logicznych (VLAN) nie mniejsza niż 4000 | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 12 | Urządzenie musi umożliwiać uruchomienie co najmniej 10 serwerów DHCP na interfejsach fizycznych oraz logicznych (VLAN). | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 13 | Obsługa DHCP Relay. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 14 | Obsługa co najmniej 10000 adresów MAC w ramach protokołu ARP. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 15 | System powinien umożliwiać pracę jako serwer VPN dla połączeń stite-to-site dla co najmniej 300 równoczesnych połączeń. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 16 | Dla VPN typu IPSec wsparcie dla protokołu IKE v1 oraz v2 oraz mechanizmów IPSec NAT Traversal, DPD, Xauth. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 17 | Wydajność IPSec VPN nie mniej niż 10Gbps. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 18 | Wydajność SSL VPN nie mniej niż 5Gbps. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 19 | System powinien umożliwiać pracę jako serwer VPN dla połączeń client-to-site dla co najmniej 1000 równoczesnych połączeń użytkowników. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 20 | W połączeniach client-to-site obsługa split tunneligu (wyznaczenie określonych sieci tunelowania). | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 21 | Dedykowany klient vpn dla systemów Windows, Linux, OSX, Adnroid, iOS. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 22 | Dedykowany klient vpn dla systemu Windows powinien posiadać ochronę antywirusową uniemożliwiającą połączenie zawirusowanych systemów. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 23 | Logowania do vpn typu Client-To-Site przy pomocy loginu i hasła, certyfikatów PKI. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 24 | Urządzenie posiada funkcję dwuskładnikowego uwierzytelniania do VPN w formie aplikacji mobilnej na systemy Android/iOS oraz w formie fizycznego tokenu. Funkcja dwuskładnikowego uwierzytelniania powinna być możliwa do zrealizowania przez dostarczone urządzenie bez konieczności instalacji dodatkowej infrastruktury serwerowej. Funkcja dwuskładnikowego dla aplikacji mobilnej dostępna również w technologii push, opartej o komunikat potwierdzenia bez konieczności przepisywania kodów uwierzytelniających. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 25 | Dostarczone 10 tokenów fizycznych, dodatkowo urządzenie musi umożliwiać wykorzystanie uwierzytelniania dwuskładnikowego w formie aplikacji mobilnej dla 90 użytkowników. Licencje jeśli są wymagane powinny być dostarczone wraz z urządzeniem. | | | | | | **Parametr wymagany**  *………………*  *ilość*  *…………………………………..*  *nazwa*  *Proszę podać ilość oraz nazwę dostarczanych licencji*  *(jeśli są wymagane)* |
| 26 | Dostęp do zasobów chronionych VPN w formie portalu obsługiwanego w całości przez przeglądarkę www w oparciu o HTML 5. Obsługa co najmniej HTTP, HTTPS, SMB/CIFS, SSH, RDP, VNC, FTP. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 27 | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 28 | Obsługa protokołów routingu RIP, OSPF, BGP. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 29 | Definiowanie routingu na pomocą polis, w szczególności na podstawie źródłowego adresu IP (PBR). | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 30 | Obsługa translacji adresów sieciowych NAT. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 31 | Firewall powinien umożliwiać detekcję aplikacji na podstawie transmitowanych danych niezależnie od danych warstwy 3/4 (porty TCP/UDP). Liczba wykrywanych aplikacji nie mniejsza niż 2000. Powinny być wykrywane również aplikacje typu malware lub botnet. Detekcja aplikacji powinna odnosić się również do aplikacji działających w oparciu o przeglądarki web (http/https).  Aplikacje powinny mieć predefiniowaną klasyfikację aplikacji poprzez poziom ryzyka i kategorie.  Urządzenie może pracować z trybie gdzie wykryta aplikacja lub ich grupa może być użyta jako klasyfikator ruchu w politykach filtracji. Przykładowo możliwość zablokowania ruchu do konkretnej aplikacji jedną regułą bez konieczności tworzenia niezależnych profili dostępu do wszystkich aplikacji i niezależnie od parametrów warstwy 3/4 jak docelowy IP lub port TCP. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 32 | Urządzenie musi mieć uruchomione zaawansowane metody filtracji ruchu w oparciu o: - kontrola aplikacji - zapobieganie zagrożeniom IPS/threat prevension - filtrowanie URL - antywirus  Jeśli powyższe elementy wymagają subskrypcji powinny one być zapewnione bez dodatkowych kosztów przez cały okres obowiązywania serwisu. Informacje dotyczące rozpoznawania nowych aplikacji, ataków, wirusów powinny być automatycznie pobierane z Internetu. Konfiguracja w.wym. elementów powinna odbywać się w zakresie konfiguracji reguł polityk firewalla. Niedopuszczalne jest konfigurowanie w.wym. elementów poprzez niezależne moduły. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 33 | Maksymalna wydajność filtracji dla uruchomionych wszystkich funkcji kontroli aplikacji, IPS, filtrowanie URL, antywirus dla rzeczywistego ruchu nie mniej niż 6Gbps.  \* [Uwaga] Oceniana będzie maksymalna wydajność filtracji firewalla w przedziale od 6Gbps do 18Gbps. Jeżeli wykonawca zaoferuje wydajność filtracji firewalla większą niż 18 Gbps to Zamawiający i tak przyjmie do porównania ofert 18 Gbps. | | | | | | **Parametr punktowany**  **…………………. Gbps**  *(podać maks. przepustowość nie mniej niż* 6Gbps*)*  Liczba punktów Wf = (Wfi/Wfmax) \* 10  gdzie:  Wfi – maksymalna wydajność filtracji firewalla w ofercie ocenianej (min. 6Gbps),  Wfmax – największa wydajność filtracji firewalla spośród wszystkich ofert ocenianych (przy czym maksymalna wartość Wfmax to 18 Gbps). |
| 34 | Mechanizm filtracji adresów URL powinien umożliwiać ze skorzystania z kategorii adresów URL udostępnionej przez producenta. Dodatkowo urządzeniu musi umożliwiać tworzenie własnych kategorii. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 35 | Filtrowanie adresów URL powinno być możliwe również dla ruchu SSL bez konieczności deszyfracji, np. poprzez inspekcję certyfikatów. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 36 | Ilość równocześnie obsługiwanych sesji TCP nie mniejsza niż 7 milionów | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 37 | Urządzenie w politykach filtrowania musi obsługiwać tzw. zdefiniowane adresy w formach: adres CIDR (IP/maska), zakres adresów IP, nazwa FQDN. Minimalna liczba obsługiwanych zdefiniowanych adresów nie mniejsza niż 20000 | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 38 | Urządzenie w politykach filtrowania musi obsługiwać grupy adresów zdefiniowanych. Grupy powinny obejmować zbiory adresów zdefiniowanych oraz inne grupy. Maksymalna liczba członków grupy nie może być niższa niż 300. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 39 | Mechanizm umożliwiający integrację z systemem Active Directory pozwalającym na ustaleniu adresów IP użytkowników zalogowanych do komputerów z sieci lokalnej i możliwości wykorzystania nazwy użytkownika w politykach filtrowania. Urządzenie musi także umożliwiać wykorzystanie grup użytkowników Active Directory. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 40 | Definiowanie polityk filtrowania ruchu w oparciu o: - strefy (zbiory interfejsów) - interfejs źródłowy - interfejs docelowy - źródłowy IP z możliwością wykorzystania zdefiniowanych adresów oraz użytkowników oraz grup użytkowników z Active Directory - docelowy IP - harmonogram czasowy - protokół (TCP/UDP) i numery portów - wykryty rodzaj aplikacji, także za pomocą zdefiniowanego poziomu ryzyka lub kategorii | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 41 | Zarządzanie urządzeniem poprzez konsolę graficzną oraz interfejs tekstowy (cli) | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 42 | Urządzenie musi umożliwiać detekcję aplikacji wykorzystywanych w transmisji sieciowej z możliwością wykorzystania tej informacji przy politykach filtrowania ruchu. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 43 | Urządzenie umożliwia deszyfrację wybranego ruchu SSL, wydajność deszyfracji nie mniej niż 7Gbps | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 44 | Monitoring (mirror) wybranego ruchu sieciowego na dedykowanym porcie | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 45 | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikacje dla funkcjonalności firewall, IPS/NGFW i SSL VPN wystawiona przez niezależną organizację certyfikującą. Organizacja powinna mieć przeprowadzone certyfikacje dla co najmniej 5 różnych producentów urządzeń typu firewall dostępnych na rynku Polskim.  Przykładowo   * ICSA dla funkcji Firewall. * ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW. * ICSA dla funkcji SSL VPN. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 46 | Urządzenie wyposażone w pamięć stałą o pojemności co najmniej 200GB pozwalające na przechowywanie logów lub przechwycony ruch (packet capture). Urządzeni powinno być odporne na awarię jednego nośnika danych. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 47 | Dostarczony system centralnego zbierania i analizy logów dla wszystkich dostarczonych urządzeń firewall (zarówno firewalli rdzeniowych oraz internetowych). System dostarczony w formie maszyny wirtualnej dla środowiska VMWare vSphere będącym w posiadaniu przez Zamawiającego lub jako urządzenie fizyczne. W przypadku urządzenia fizycznego system powinien być odporny na awarie jednego dysku.  Oprogramowanie powinno umożliwiać w graficznej formie przegląd i filtrowanie ruchu w czasie rzeczywistym obejmujący wszystkie aspekty filtrowania (firewall, IPS, URL filtering, antywirus). Zakres filtrowania powinien obejmować co najmniej elementy (adres źródłowy, docelowy, zakres czasowy, porty TCP/UDP URL, kategoria URL, aplikacja, kategoria aplikacji). Możliwość wykorzystania w filtrach wyrażeń regularnych.  Możliwość zapisania co najmniej 3TB logów. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 48 | Wykonawca zamontuje oraz wstępnie skonfiguruje urządzenie zgodnie z ustaleniami z Zamawiającym. Dostarczone urządzenia powinny zostać skonfigurowane do pracy w trybie wysokiej dostępności. Awaria lub wyłączenie jednego urządzenia nie powoduje przestoju w pracy sieci komputerowej. Dodatkowo Wykonawca dokona migracji konfiguracji z zachowaniem wszystkich funkcjonalności z urządzenia Fortigate FG-600D obecnie używanego przez Zamawiającego oraz przełączy urządzenie obecnie używane na dostarczone. Czas przestoju pracy sieci komputerowej podczas przełączenia nie może byś dłuższy niż 2h. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 49 | Wyznaczonych trzech pracowników zostanie przeszkolonych z obsługi urządzenia w ramach autoryzowanego szkolenia producenta. Szkolenie powinno odbywać się w języku polskim w miejscowości Zamawiającego i trwać nie krócej niż 3 dni.  Dopuszcza się spełnienie tego wymogu szkoleniem zaoferowanym dla firewalla rdzeniowego o ile będzie ono identyczne co do zakresu szkoleniowego. | | | | | | **Parametr wymagany**  *(nie wypełniać)* |
| 50 | Gwarancja oraz Wsparcie techniczne dla produktu co najmniej 36 miesięcy. Serwis dostępny w trybie 24x7 przez 365 dni w roku. Wymiana uszkodzonego sprzętu w siedzibie zamawiającego najpóźniej następnego dnia roboczego. W cenie dostawy przedmiotu umowy dostęp do aktualizacji oprogramowania systemowego w trakcie trwania kontraktu serwisowego. Wsparcie techniczne dla firewalli rdzeniowych oraz firewalli internetowych muszą być realizowane przez jeden podmiot.  \* [Uwaga] Oceniana będzie całkowita liczba miesięcy w przedziale od 37 miesięcy do 72 miesięcy. Jeżeli wykonawca zaoferuje okres gwarancji i wsparcia technicznego dłuższy niż 72 miesiące, to Zamawiający i tak przyjmie do porównania ofert okres 72 miesięcy. | | | | | | **Parametr oceniany**  **Podać okres trwania gwarancji i wsparcia technicznego**  **………………………………..miesięcy**  **(podać okres w pełnych miesiącach na jaki zostanie udzielona gwarancja i wsparcie techniczne – min. 36 miesięcy)**  Liczba punktów Gw = (Gwi/Gwmax) \* 20  gdzie:  Gwi – liczba miesięcy gwarancji i wsparcia technicznego w ofercie ocenianej (min. 37 miesięcy),  Gwmax – największa liczba miesięcy gwarancji i wsparcia technicznego spośród wszystkich ofert ocenianych (przy czym maksymalna wartość Gwmax to 72 miesięcy). |