**Załącznik nr 2.1 do SWZ**

 **FZ- 2380/22/24/ET**

**CZĘŚĆ 1**

**Przełączniki sieciowe wraz z ukompletowaniem x 10 kpl.**

1. Typ i liczba portów: 48 porty 10/100/1000BaseT RJ-45 POE + uplink 4x10G SFP
2. Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek: Gigabit Ethernet 1000Base-T, Gigabit Ethernet 1000Base-SX, Gigabit Ethernet 1000Base-LX/LH, Gigabit Ethernet 1000Base-EX, Gigabit Ethernet 1000Base-ZX, Gigabit Ethernet 1000Base-BX-D/U, 10Gigabit Ethernet 10GBase-SR, 10Gigabit Ethernet 10GBase-LR, 10Gigabit Ethernet 10GBase-ER, 10Gigabit Ethernet 10GBase-ZR, 10Gigabit Ethernet typu twinax, DAC (SFP+ - SFP+) Typ portu POE+
3. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:

Przepustowość w ramach stosu - 80Gb/s,

8 urządzeń w stosie,

Zarządzanie poprzez jeden adres IP,

Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

1. Zasilanie i chłodzenie:

Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco" - ang. hot swap),

Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia, Redundantne wentylatory,

1. Parametry wydajnościowe:

Przepustowość przełącznika (switching capacity): 176 Gb/s (bez podłączenia do stosu), 256 Gb/s (z podłączeniem do stosu),

Prędkość przesyłania (forwarding rate): 130.95 Mpps Bufor pakietów - min. 6MB Pamięć DRAM - min. 2GB Pamięć flash - min. 4GB Obsługa: 500 aktywnych sieci VLAN 16000 adresów MAC 3000 tras IPv4 1500 tras IPv6 Ilość wpisów w listach kontroli dostępu Security ACL - 1000 ilość wpisów w listach kontroli dostępu QoS ACL - 1000 512 interfejsów SVI L3 Jumbo frame 9198B

48 połączeń zagregowanych typu „port channel" 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP

1. Obsługa protokołu NTP
2. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
3. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: IEEE 802.1w Rapid Spanning Tree Per-VLAN Rapid Spanning Tree (PVRST+) IEEE 802.1s Multi-Instance Spanning Tree Obsługa 64 instancji protokołu STP
4. Obsługa protokołu LLDP i LLDP-MED.
5. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
6. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
7. Możliwość uruchomienia funkcji serwera DHCP
8. Mechanizmy związane z bezpieczeństwem sieci:

Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,

Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,

Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,

Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,

Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania -802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),

Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,

Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) - w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),

Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,

Obsługa list kontroli dostępu (ACL) następujących typów:

Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,

VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,

Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,

Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach
i dniach tygodnia);

Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128)
z mechanizmem MACsec Key Agreement (MKA),

Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP - Control Plane Policing),

Funkcja Private VLAN;

1. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna ekwencja uruchamiania, Sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
2. Mechanizmy związane z zapewnieniem jakości usług w sieci:

Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, implementacja algorytmu Shaped Round Robin dla obsługi kolejek,

 Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,

Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),

Kontrola sztormów dla ruchu broadcast/multicast/unicast,

Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP - poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

1. Obsługa protokołów i mechanizmów routingu:

Routing statyczny dla IPv4 i IPv6, Routing dynamiczny - RIP, OSPF do 1000 wpisów ,

PIM Stub do 1000 wpisów,

Policy-based routing (PBR),

Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,

Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

1. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego - mechanizmy SPAN, RSPAN
2. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),
3. Funkcjonalność sondy IP SLA Responder,
4. Zarządzanie:

Port konsoli, Dedykowany port Ethernet do zarządzania out-of-band,

Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,

Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,

Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, Wsparcie dla protokoły RESTCONF,

Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,

Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,

Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,

Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;

1. Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU,
2. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow - obsługa 16000 strumieni (flow),
3. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow - obsługa 32000 strumieni (flow),
4. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,
5. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
6. Możliwość enkapsulacji ruchu w pakiety VXLAN,
7. Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci,
8. Przełącznik wyposażony w możliwość zasilania urządzenia zewnętrznego z portów RJ45 w standardzie PoE+ gdzie łączna moc urządzeń podłączonych do przełącznika w standardzie PoE+ nie mniejsza niż 740W,
9. Dla każdego z **10 switch'y** jako wyposażenie należy dostarczyć:

Przełącznik wyposażony w zasilacz podstawowy oraz dodatkowy zasilacz zapasowy o mocy analogicznej do mocy zasilacza podstawowego,

Przełącznik wyposażony w następujące wkładki interfejsowe:

SFP-10G-SR: 4szt,

1. Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres min. 3 lat, oraz gwarancję producenta utrzymaną w reżimie 8x5xNBD przez okres min. 3 lat.
2. Przełączniki wyposażone w moduły wraz z okablowaniem do łączenia w stos gdzie zamawiający przewiduje utworzenie trzech stosów:
3. stosu składającego się z 3 przełączników umieszczonych w jednej szafie rack, gdzie każdy z przełączników jest oddzielony od siebie organizerem przewodów 1U,
4. stosu składającego się z 4 przełączników umieszczonych w jednej szafie rack, gdzie każdy z przełączników jest oddzielony od siebie organizerem przewodów 1U,
5. stosu składającego się z 3 przełączników gdzie dwa przełączniki znajdują się
w jednej szafie oddzielone od siebie organizerem przewodów 1U, natomiast trzeci przełącznik znajdować się będzie w odrębnej szafie oddalonej >1.5m,
6. Dodatkowy przewód stakujący do zaoferowanych przełączników o długości minimum 3m.
w ilości 2 szt.
7. Dodatkowy patchcord o długości nie mniej niż 3.0m do ww. wkładek w ilości 8 szt.

**Załącznik nr 2.2 do SWZ**

 **FZ- 2380/22/24/ET**

**CZĘŚĆ 2**

**Urządzenia NG firewall – 1 kpl.**

1. Musi to być specjalizowane urządzenie sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby, Active/Active. Wymagana całość sprzętu i oprogramowania musi być dostarczona i zapewniać wsparcie serwisowe przez jednego tego samego producenta.
2. Urządzenie musi umożliwiać działanie w następujących trybach pracy:
	1. rutera (tzn. w warstwie 3 modelu ISO OSI),
	2. mostu (tzn. w warstwie 2 modelu ISO OSI),
	3. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary.).
	4. w trybie pasywnego nasłuchu (tzw. sniffer/tap).

System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.

1. Urządzenie musi być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden dedykowany port zarządzający realizowany jako port Ethernet 10/100/1000 lub jako port SFP z wkładką 1000BASE-T.
2. Urządzenie musi być wyposażone w minimum 2 zasilacze typu AC 230V pracujące redundantnie.
3. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
4. Urządzenie firewall musi posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw. management plane). Akceptowana jest separacja logiczna zasobów zrealizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU cores) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji.
5. Urządzenie firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać min. 4000 znaczników VLAN.
6. Urządzenie firewall musi wspierać protokół LACP.
7. Urządzenie firewall musi zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
8. Urządzenie firewall musi działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
9. Polityka zabezpieczeń firewall musi uwzględniać
	1. adresy IP źródłowe i docelowe,
	2. protokoły i usługi sieciowe,
	3. aplikacje,
	4. kategorie URL,
	5. użytkowników aplikacji i grupy,
	6. reakcje zabezpieczeń,
	7. logowanie zdarzeń (początek i koniec sesji)
	8. strefa wejściowa i wyjściowa
10. Urządzenie firewall musi automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3500 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz z aplikacjami przemysłowymi (tzw. ICS/OT) np. DNP3, Modbus.

Urządzenie musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).

1. Urządzenie firewall musi pozwalać na blokowanie transmisji plików wybranego typu, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.
2. Urządzenie firewall musi być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
3. Urządzenie firewall musi być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy przewidzieć odpowiednie licencje dla minimum 30 administratorów na wszystkie oferowane urządzenia.
4. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
5. Urządzenie firewall musi umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH.
6. Urządzenie firewall musi zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
	1. Microsoft Active Directory,
	2. Microsoft Exchange
	3. Terminal Services
	4. Syslog
	5. Cisco ISE
7. Polityka kontroli dostępu (urządzenia firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.
8. Urządzenie firewall musi pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL, połączeniach VPN.
9. Urządzenie firewall musi umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
10. Urządzenie firewall musi umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
	1. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
	2. API
11. Urządzenie firewall musi posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESXi i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.
12. Urządzenie firewall musi obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.
13. Urządzenie firewall musi obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
14. Urządzenie firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
15. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami informacji o NAT.
16. Urządzenie firewall musi pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.
17. Urządzenie firewall musi obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
18. Urządzenie firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.
19. Urządzenie firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS który nie ma zostać odszyfrowany, ale poddany sprawdzeniu czy certyfikat serwera nie wygasł oraz sprawdzeniu czy certyfikat nie pochodzi od zaufanego wystawcy. W takim przypadku urządzenie musi umożliwiać blokadę takiej sesji użytkownika.
20. Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
21. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL (w przypadku, gdy jest wymagane jego dostarczenie) albo możliwość wykorzystania własnej utworzonej na urządzeniu listy URL które mają podlegać deszyfracji albo być z niej wykluczone (tzw. wyjątek).
22. Urządzenie firewall musi posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
23. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów:TLS\_AES\_128\_GCM\_SHA256, TLS\_AES\_256\_GCM\_SHA384, TLS\_CHACHA20\_POLY1305\_SHA256.
24. Urządzenie firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.
25. Urządzenie firewall musi wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.
26. Urządzenie firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).
27. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
28. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
29. Urządzenie firewall musi zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.
30. Urządzenie firewall musi obsługiwać funkcję DNS proxy.
31. Urządzenie firewall musi obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowania klienta Remote Access VPN dla laptopów z systemem klienckim Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną ilość dla oferowanego typu urządzeń.
32. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
33. Urządzenie firewall dla zdalnego dostępu VPN muszą umożliwiać następujące funkcjonalności:
	1. Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN)
	2. Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS i Google Android.
	3. Dostępność oprogramowania klienckiego VPN dla urządzeń mobilnych z systemami: Apple iOS (10-16), Android (6-13), Win UWP
	4. Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 8-11; Windows 10 UWP; iOS 10-14; MacOS 10.15-13; Google Android 6-11; Linux CentOS, RHEL, Ubuntu;
	5. Sprawdzanie informacji o systemie operacyjnym, aktualizacji poprawek OS, aktualizacji oprogramowania antywirusowego itp. dla systemów Windows.
	6. Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów Windows.
	7. Możliwość pomijania tunelu zdalnego dostępu VPN dla specyficznych aplikacji, domeny DNS, aplikacji video. Dla podłączających się stacji/laptopów Windows i MacOS.
	8. Dodatkowa identyfikacja urządzeń użytkownika na bazie unikalnego identyfikatora innego niż adres IP (Windows – MachineGuid, Android – Android ID, iOS – UDID) pozwalająca na blokadę dostępu VPN dla wybranego urządzenia. Np. blokada dostępu VPN dla urządzenia zainfekowanego.
34. Producent oferowanego rozwiązania musi być obecny w najnowszym rynkowym raporcie Gartner Magic Quadrant for Enterprise Network Firewalls w części (tzw. ćwiartce) Leaders.
35. Dostarczane razem z urządzeniami subskrypcje, licencje, gwarancje muszą funkcjonować przez okres **36** miesięcy. Dostępność wsparcia PREMIUM – czas reakcji poniżej 1 godziny, dostawa części i wymiana sprzętu w następnym dniu roboczym, dostępność powyższego na 24/7/365.
36. W przypadku potrzeby wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby dyski zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji.

**Wymagania dodatkowe dla urządzeń NG Firewall.**

Należy dostarczyć 1 szt. urządzenia

Razem z urządzeniem muszą zostać dostarczone następujące typy i ilości modułów połączeniowych.

1. Do LAN**: 4** szt. SFP+ 10GE wariant SR wraz z patchcord-em 3m.

Urządzenie musi, spełniać dodatkowo wymagania:

1. Urządzenie musi być wyposażone w minimum:
	1. minimum 8 porty Ethernet RJ45 wspierających 100Mbps/1GE;
	2. minimum 4 porty Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps;
	3. minimum 4 porty Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps z zasilaniem PoE
	z budżetem 150W mocy oraz możliwością udostępnienia na porcie 50W mocy;
	4. minimum 6 portów Ethernet SFP (akceptujących moduły 1GE SFP)
	5. minimum 4 portów Ethernet SFP+ (akceptujących moduły 10GE SFP+ oraz 1GE SFP)
	6. minimum 1 port dla celów połączenia urządzeń w HA: minimum 1x 10GE SFP+ (lub szybszy) oraz minimum 2x 1GE (SFP lub RJ45) (lub szybszy). Porty te muszą być traktowane jako dodatkowe względem wymaganych powyżej. Nie dopuszcza się liczenia jako HA, portów wymaganych wcześniej.
2. Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 120 GB na potrzeby systemu operacyjnego i logów.
3. W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasób dyskowy zostały wymontowany z urządzenia i pozostał w jego siedzibie w celu bezpiecznej utylizacji.
4. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
	1. Minimum 8.1 Gbps dla rozpoznawania i kontroli aplikacji,
	2. Minimum 3,8 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antyspyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.
	3. Minimum 4.5 Gbps wydajności IPSec VPN.
	4. Minimum 90 000 nowych sesji na sekundę.
	5. Minimum 845,000 równoległych sesji
	6. Minimum 1500 tuneli klienckich VPN
	7. Minimum 2500 sąsiedztw IKE (IPSec)
5. Musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia.
6. Musi umożliwiać zdefiniowanie nie mniej niż 1500 reguł polityki bezpieczeństwa oraz 3000 reguł NAT.
7. Urządzenie musi być wyposażone w minimum 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
8. Urządzenie musi być przeznaczone do montażu w szafie Rack 19”.
9. Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
10. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
11. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
12. Urządzenie musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny (nie rzadziej niż raz na 48h) i pochodzić od tego samego producenta co firewall.
13. Urządzenie musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
14. Urządzenie musi posiadać funkcję filtrowania URL.
15. Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.
16. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
17. Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen.
18. Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.
19. Urządzenie musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sandbox” plików różnych typów (Windows Portable Executable (m.in. exe, dll), MacOS (MachO, DMG, PKG), Linux ELF, pdf, MS Office, JAR, APK, JS, VBS, PowerShell Script, HTA) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Interwał aktualizacyjny to maksymalnie 2 godziny.
20. Administrator musi mieć możliwość konfiguracji jakiego rodzaju typy plików z listy wspieranych przez funkcję Sandbox zostaną wysłane do skanowania przez „Sandbox”.
21. Musi istnieć możliwość wysyłania plików do systemu Sandbox w chmurze obliczeniowej producenta oraz do fizycznych (lokalnych) urządzeń Sandbox gdyby takie zostały zainstalowane w przyszłości w sieci Zamawiającego.
22. Urządzenie musi wykrywać i blokować zagrożenia DNS w ruchu przechodzącym przez urządzenie bez potrzeby rekonfiguracji serwera DNS i bez potrzeby ustawiania firewall jako serwera DNS. Wykrywający i blokujący ruch do domen uznanych za złośliwe musi być sterowany (przekierowanie) za pomocą funkcji DNS Sinkholing.
23. Urządzenia muszą posiadać ciągły (on-line) dostęp do centralnego repozytorium zagrożeń DNS, który będzie wykorzystywany w procesie decyzyjnym ochrony DNS.
24. Urządzenie musi zabezpieczać działania protokołu DNS poprzez procesowanie zapytań DNS w celu wykrywania i blokowania:
	1. wykrywanie domen dynamicznych Dynamic DNS;
	2. wykrywanie zapytań do domen złośliwych;
	3. wykrywanie domen generowanych przez algorytmy DGA;
	4. wykrywanie tunelowania złośliwej komunikacji w protokole DNS;
	5. wykrywanie DNS Exfiltration or DNS Inflitration;

**Załącznik nr 2.3 do SWZ**

 **FZ- 2380/22/24/ET**

**CZĘŚĆ 3**

**Punkty dostępowe – 12 szt.**

1. Punkt dostępowy o wymiarach ø220 x 48mm i wadze 960g bez dodatkowego zestawu montażowego lub 1090g łącznie z zestawem montażowym.
2. Obudowa z tworzywa sztucznego posiadająca stalowe punkty montażowe.
3. Interfejs sieciowy typu RJ45 w technologii 2.5GbE z możliwością zarządzania z poziomu ethernet oraz z poziomu bluetooth.
4. Punkt dostępowy musi posiadać możliwość zarządzania centralnego zarówno z poziomu dedykowanego urządzenia lub wirtualnej maszynie z systemem (Linux, Windows).
5. Oferowane zarządzanie centralne musi posiadać funkcje takie, jak: monitorowanie statystyk ruchu w czasie rzeczywistym, ich analizę poprzez wbudowane narzędzia wizualizacji danych, uwierzytelnianie gości za pomocą strony powitalnej, aktualizacja i restart systemu oraz łatwe skalowanie sieci.
6. Punkt dostępowy powinien obsługiwać technologię zasilania w standardzie PoE+.
7. Urządzenie powinno wspierać standard zasilania PoE oraz mieć możliwość zasilania
z zewnętrznego źródła zasilania o parametrach 48V, 0.5A.
8. Punkt dostępowy powinien mieć możliwość pracy w zakresie napięć 44 - 57V DC
o maksymalnym poborze mocy 22W.
9. Punkt dostępowy powinien charakteryzować się poniższymi parametrami pracy:

**Maksymalna moc nadawcza dla poszczególnych pasm:**

2.4 GHz – 22 dBm,

5 GHz – 26 dBm,

6 GHz – 26 dBm.

**Praca w techonologii MIMO (Multiple Input Multliple Output) w poszczególnych pasmach:**

2.4 GHz – 2 x 2 (UL MU-MIMO),

5 GHz – 4 x 4 (DL/UL MU-MIMO),

6 GHz – 4 x 4 (DL/UL MU-MIMO).

**Minimalna przepustowość pasm:**

2.4 GHz 573.5 Mbps,

5 GHz 4.8 Gbps,

6 GHz 4.8 Gbps.

**Zysk anten dla pracy w pasmach:**

2.4 GHz – 3.2 dBi,

5 GHz – 5.3 dBi,

6 GHz – 6 dBi.

1. Punkt dostępowy powinien posiadać fizyczny przycisk przywracania do ustawień fabrycznych tzw. „reset”.
2. Urządzenie powinno posiadać stalowy (SUS304) zestaw montażowy za pomocą którego można podwiesić je pod sufitem lub przytwierdzić do ściany.
3. Urządzenie powinno być przystosowane do pracy w warunkach otoczenia, którego temperatura znajduje się w przedziale od -30 do 60 °C oraz w przedziale wilgotności od 5% do 95%.
4. Urządzenie powinno obsługiwać standardy pracy sieci WiFi takie jak 802.11a/b/g/n/ac/ax (WiFi 6/6E).
5. Urządzenie powinno wspierać mechanizmy związane z bezpieczeństwem sieci WiFi takie jak WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3).
6. Urządzenie powinno umożliwiać utworzenie 8 BSSID na każde z pasm pracy tj. 2.4 GHz, 5 GHz, 6 GHz.
7. Punkt dostępowy powinien wspierać obsługę VLAN w standardzie 802.1Q.
8. Punkt dostępowy powinien posiadać możliwość zarządzania przepustowością łącza dla danego klienta tj. Advanced QoS.
9. Punkt dostępowy powinien umożliwiać izolację podłączonych urządzeń.
10. Punkt dostępowy powinien obsługiwać równolegle nie mniej niż 590 podłączonych urządzeń.
11. Punkt dostępowy powinien posiadać funkcjonalność polegającą na możliwości kontrolowania zakresu częstotliwości przez stację bazową WiFi pod kątem użytkowników priorytetowych tzw. Zero Wait DFS.
12. Urządzenie powinno obsługiwać poniższe prędkości dla poszczególnych standardów:
* 802.11a – 6, 9, 12, 18, 24, 36, 48, 54 Mbps,
* 802.11b – 1, 2, 5.5, 11 Mbps,
* 802.11g – 6, 9, 12, 18, 24, 36, 48, 54 Mbps,
* 802.11n (WiFi 4) – 6.5 Mbps to 600 Mbps (MCS0 – MCS31, HT 20/40),
* 802.11ac (WiFi 5) – 6.5 Mbps to 3.4 Gbps (MCS0 – MCS9 NSS1/2/3/4, VHT 20/40/80/160),
* 802.11ax (WiFi 6/6E) 7.3 Mbps to 4.8 Gbps (MCS0 – MCS11 NSS1/2/3/4, HE 20/40/80/160).

20. Punkt dostępowy powinien pokrywać swym zasięgiem obszar o powierzchni nie mniej niż 135 m2 .

21. Każdy z dostarczonych punktów dostępowych musi posiadać 24 miesiące gwarancji.