**Załącznik nr 1 do Umowy**

**Rozbudowa istniejącej infrastruktury urządzeń brzegowych WAN Sieci Badawczej Łukasiewicz**

**Opis Przedmiotu Zamówienia**

Spis treści

[I. Przedmiot Zamówienia – wstęp 3](#_Toc141368711)

[II. Wymagania dotyczące dostarczanych urządzeń klasy Next Generation Firewall 3](#_Toc141368712)

[II.1 Wymagania ogólne 3](#_Toc141368713)

[II.2 Funkcje podstawowe NGFW 4](#_Toc141368714)

[II.3 Funkcje bezpieczeństwa NGFW 6](#_Toc141368715)

[II.4 Dostęp zdalny VPN dla użytkowników 7](#_Toc141368716)

[II.5 Redundancja, monitoring i wykrywanie awarii 7](#_Toc141368717)

[II.6 Wymagania dla połączeń Site to Site VPN (parametry IPsec) 7](#_Toc141368718)

[II.7 Szczegółowe wymagania fizyczne oraz wydajnościowe NGFW 9](#_Toc141368719)

[II.8 Zgodność urządzeń z Centralnym Systemem Zarządzania (CSZ) 14](#_Toc141368720)

[II.9 Współpraca nowych urządzeń NGFW z posiadanymi obecnie przez Zamawiającego 15](#_Toc141368721)

[III. Dokumentacja przedwdrożeniowa 15](#_Toc141368722)

[IV. Wymagania dotyczące instalacji dodatkowych urządzeń w sieci WAN Zamawiającego 16](#_Toc141368723)

[V. Wymagania dotyczące gwarancji (usuwanie awarii) 17](#_Toc141368724)

[VI. Wymagania dotyczące wsparcia powdrożeniowego 17](#_Toc141368725)

#

# Przedmiot Zamówienia – wstęp

1. Wykonawca rozbuduje istniejący system urządzeń brzegowych sieci WAN Zamawiającego poprzez:
* dostawę nowych urządzeń firewall współpracujących z Centralnym Systemem Zarzadzania (Forcepoint SMC) oraz wkładek światłowodowych
* instalację i integrację nowych urządzeń z posiadanym obecnie przez Zamawiającego Systemem Centralnego Zarządzania (Forcepoint SMC), na zasadach określonych w OPZ i projekcie umowy.
1. Główne elementy zamówienia:
	1. Dostawa urządzeń klasy Next Generation Firewall (NGFW) z niezbędnym oprogramowaniem, licencjami/subskrypcjami, oraz wsparciem technicznym:
		* Urządzenia wysokiej wydajności 1 sztuka
		* Urządzenia średniej wydajności 10 sztuk (w tym urządzenie zapasowe)
		* Urządzenia niskiej wydajności 7 sztuk (w tym urządzenie zapasowe)

oraz dostawa wkładek światłowodowych kompatybilnych z dostarczanymi urządzeniami (NGFW):

* + - Wkładki światłowodowe SFP 1Gb SM 7 sztuk
		- Wkładki światłowodowe SFP+ 10Gb SM 8 sztuk
		- Wkładki światłowodowe SFP+ 10Gb MM 4 sztuk
	1. Dokumentacja przedwdrożeniowa
	2. Instalacja, konfiguracja oraz integracja nowych urządzeń z istniejącymi urządzeniami oraz z Centralnym Systemem Zarządzania posiadanym przez Zamawiającego (Forcepoint SMC)
	3. Wsparcie techniczne oraz objęcie nowych urządzeń gwarancją
	4. Wsparcie powdrożeniowe w ilości 150 godzin konsultacji

#  Wymagania dotyczące dostarczanych urządzeń klasy Next Generation Firewall

Urządzenia NGWF muszą być zarządzane z poziomu Centralnego Systemu Zarządzania (Forcepoint SMC) oraz spełniać niżej wymienione warunki:

* spełniać wymagania ogólne,
* realizować funkcjonalności podstawowe NGFW,
* realizować wymagane funkcje bezpieczeństwa NGFW,
* realizować dostęp zdalny VPN dla użytkowników,
* spełniać wymagania dotyczące redundancji i monitoringu oraz wykrywania awarii,
* spełniać wymagania dotyczące realizowania połączeń VPN,
* spełniać szczegółowe wymagania fizyczne i wydajnościowe,
* spełniać wymagania zgodności i integracji z Systemem Centralnego Zarządzania,
* współpracować z urządzeniami posiadanymi obecnie przez Zamawiającego.

# Wymagania ogólne

1. Dostarczane urządzenia muszą być fabrycznie nowe (urządzenia nie mogą być refabrykowane) i wyprodukowane nie wcześniej niż 12 miesięcy przed dostawą.
2. W terminie składania ofert urządzenia nie powinny być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży. Urządzenia powinny mieć zapewnione wsparcie producenta przez okres min. 5 lat od upływu terminu składania ofert.
3. Dostarczane urządzenia muszą być wyposażone we wszystkie komponenty software’owe, jak oprogramowanie, licencje, subskrypcje i inne niezbędne do prawidłowego działania urządzeń.
4. W przypadku modeli urządzeń przystosowanych do montażu w szafach 19’’, konieczne jest dostarczenie niezbędnych akcesoriów do ich montażu.
5. Urządzenia muszą być przystosowane do zasilania AC 230V, 50Hz.
6. Średnia konsumpcja energii elektrycznej przez urządzenie to nie więcej niż 50W a maksymalna konsumpcja nie więcej niż 65W.
7. Urządzenia mogą pracować przy względnej wilgotności powietrza pomiędzy 20% a 80%.
8. Urządzenia mogą pracować w temperaturze od 5 do 35 stopni Celsjusza.
9. Urządzenia muszą być zgodne z normą Unii Europejskiej EN55032 dotyczącą kompatybilności elektromagnetycznej.
10. Przewody zasilające muszą być kompatybilne z gniazdem elektrycznym Typ IEC C13 lub CEE7/7 i mieć długość nie mniejszą niż 1,5 metra. Liczba przewodów zasilających ma odpowiadać liczbie zasilaczy w urządzeniach.
11. Zamawiający wymaga, aby wszystkie miejsca (sloty) urządzeń przeznaczone na montaż zasilaczy, były wyposażone w zasilacze.
12. Zamawiający wymaga, aby wszystkie dostarczane urządzenia miały możliwość aktywowania wszystkich funkcjonalności wyszczególnionych w punkcie *II.3 Funkcje Bezpieczeństwa*, a więc posiadały wsparcie sprzętowe, systemowe oraz licencje i subskrypcje, a także wszystkie inne komponenty i składniki umożliwiająceZamawiającemuuruchomienie każdej z tych funkcjonalności bez konieczności wymiany urządzenia na inną wersję sprzętową, ani wykonania zmiany oprogramowania systemowego, ani wykonania dodatkowych zakupów
13. Wszystkie wyżej wymienione wymagania muszą być spełnione od dnia podpisania umowy.

# Funkcje podstawowe NGFW

1. Możliwość uruchomienia w jednym z dwóch trybów:
	1. Routera z funkcją NAT, pracującego w warstwie L3 modelu OSI.
	2. Transparentnym, pracującego w warstwie L2 modelu OSI.
2. Możliwość tworzenia stref bezpieczeństwa (ang. Security Zones).
3. Realizacja polityk bezpieczeństwa w oparciu o następujące kryteria:
	1. Źródłowa lub docelowa strefa bezpieczeństwa.
	2. Źródłowy lub docelowy adres/obiekt IPv4 lub IPv6.
	3. Aplikacja (w oparciu o sygnatury).
	4. Serwis (dowolna, możliwa kombinacja port/protokół).
	5. Protokół.
	6. Grupa Aplikacji.
	7. Grupa Protokołów.
	8. Użytkownik lub grupa użytkowników.
	9. Geolokację.
	10. Nazwy domen.
	11. Listy adresów IP oraz URL.
	12. Czas realizacji polityki.
4. Translacja adresów (NAT) dla IPv4 oraz IPv6 w tym dla IPv6 realizację co najmniej:
	1. NAT64 (RFC 6146) co najmniej dla TCP i UDP
	2. 464XLAT CLAT (RFC 6877)
	3. SIIT EAM (RFC 7757)
5. Agregowanie połączeń fizycznych zgodne ze standardem IEEE 802.3ad.
6. Obsługa subinterfejsów VLAN-IEEE 802.1q w ilości nie mniej niż 4094.
7. Obsługa wirtualnych tablic routingu:
	1. Realizacja wirtualnych systemów / wirtualnych kontekstów funkcjonujących w ramach fizycznego urządzenia firewall dostarczonego przez producenta.
	2. Realizacja wirtualizacji w obrębie urządzenia fizycznego musi być realizowana w oparciu o rozwiązanie dostarczone przez producenta i nie może wymagać instalowania oprogramowania firm trzecich.
	3. Możliwość uruchomienia co najmniej 3 wirtualnych kontekstów w ramach urządzenia, bez dodatkowej licencji.
8. Obsługa Routingu statycznego oraz Policy Based Routingu (PBR).
9. Synchronizacja czasu z serwerem NTP.
10. Kontrola pasma oraz ruchu (Quality of Service, QoS).
11. Obsługa protokołów routingu dynamicznego (co najmniej BGP, OSPFv2 i OSPFv3 oraz PIM).
12. Obsługa SSH w wersji 2.
13. Obsługa SNMP v2c/v3 wraz z SNMP Traps.
14. Obsługa SYSLOG dla przynajmniej dwóch adresów docelowych jednocześnie.
15. Obsługa LLDP (Link Layer Discovery Protocol IEEE 802.1ab).
16. Obsługa protokołu DHCP (w trybach, Server, Relay).
17. Dedykowany dla zarządzania port konsolowy Rj45.
18. Urządzenie posiada co najmniej 1 port USB.
19. Obsługa połączeń szyfrowanych IPSec VPN oraz SSL VPN.
20. Realizacja funkcjonalności SD-WAN:
	1. Rozwiązanie musi być dostarczone z pełnym kompletem funkcjonalności SD-WAN oferowanym przez producenta rozwiązania i uruchomienie jakiejkolwiek funkcjonalności SD-WAN nie będzie wymagało zakupu jakichkolwiek dodatkowych licencji.
	2. Możliwość sterowania ruchem aplikacji sieciowych w obrębie wielu łącz pomiędzy lokalizacjami z uwzględnieniem parametrów jakościowych oferowanych przez poszczególne łącza w tym: utraty pakietów czy opóźnień.
21. W przypadku utraty łączności z Centralnym Systemem Zarządzania, urządzenie musi być autonomiczne (poprawne uruchomienie i praca po restarcie urządzenia).
22. Rozwiązanie powinno wspierać technologię dwu-składnikowego uwierzytelniania dla administratorów NGFW oraz połączeń VPN client-to-site.
23. NGFW musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

# Funkcje bezpieczeństwa NGFW

1. IPS (Ochrona przed zagrożeniami)
	1. Inspekcja ruchu (IPS) w oparciu o sygnatury dostarczane przez producenta rozwiązania (producent musi udostępniać bazę minimum 16000 sygnatur dla urządzenia).
	2. Rozwiązanie musi realizować funkcję „blacklist” umożliwiającą całkowite (dowolny port i protokół) zablokowanie ruchu z adresu IP (blokowanie musi być realizowane przez system IPS i być wynikiem ataku przeprowadzonego z danego adresu, wykrytego przez silnik IPS, lub też informacji dostarczanej w postaci sygnatury przez producenta rozwiązania).
	3. Możliwość ręcznego tworzenie sygnatur dla wszystkich silników IPS działających na rozwiązaniu.
	4. Rozwiązanie musi umożliwić takie przygotowanie polityki, aby system wykrywał atak w oparciu o sygnaturę i wskazywał, że ruch ten powinien być blokowany, ale jednocześnie nie blokował ruchu, a jedynie informował o zaistniałym zdarzeniu.
	5. Rozwiązanie musi umożliwić pisanie wyjątków od polityki dotyczących pojedynczych sygnatur dla pojedynczych hostów (adresów IP).
2. User Identity (identyfikacja użytkowników)
3. Integracja z usługami katalogowymi w tym w szczególności z Microsoft Active Directory.
4. Budowanie polityk dostępowych w oparciu o konta użytkowników oraz grupy w Microsoft Active Directory.
5. Możliwość instalacji agenta na komputerach z systemem Microsoft Windows w celu rozpoznawania użytkowników i mapowania ich do adresu IP. W szczególności na serwerach realizujących usługi terminalowe.
6. Możliwość generowania raportów z aktywności pojedynczego użytkownika dotyczących między innymi:
	* + aktywności sieciowej (połączenia sieciowe),
		+ ilości transferowanych danych,
		+ wykorzystywanych aplikacji sieciowych,
7. Zbieranie informacji dotyczącej stanu systemu operacyjnego na którym pracuje użytkownik w celu realizacji polityk dostępowych. Dane powinny zawierać między innymi informacje o:
	* + wersji systemu operacyjnego,
		+ stanie aktualizacji systemu operacyjnego,
		+ stanie oprogramowania antywirusowego,
		+ stanie usługi firewall.
8. Application Control (kontrola aplikacji)
	1. Identyfikacja aplikacji niezależnie od wykorzystywanego portu TCP/UDP na podstawie dostarczonych przez producenta sygnatur aplikacji (co najmniej 7000 aplikacji w tym aplikacji chmurowych, niezależnie od portu, na którym działa usługa).
	2. Baza aplikacji musi być automatycznie aktualizowana w formie aktualizacji dostarczanych przez producenta oprogramowania.
	3. Rozwiązanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji, które ma rozpoznawać Firewall.
9. Antitvirus & Malware Protection (ochrona antywirusowa i kontrola plików)
	1. Urządzenie musi posiadać możliwość realizowania kontroli antywirusowej plików w oparciu o minimum dwa mechanizmy:
		* Sygnaturowy silnik AV działający na urządzeniu
		* Mechanizm kontroli plików na podstawie ich reputacji
	2. Polityka filtrowania AV musi umożliwiać wykorzystanie różnych mechanizmów skanowania lub poziomu skanowania w zależności od rodzaju pliku (MIME).
	3. Rozwiązanie musi umożliwić integrację z rozwiązaniem typu DLP w oparciu o protokół ICAP.
10. HTTPS Inspection (inspekcja ruchu szyfrowanego)

# Dostęp zdalny VPN dla użytkowników

1. Urządzenie musi umożliwić realizację klienckich połączeń zdalnych przy wykorzystaniu IPsec VPN oraz SSL VPN (w tym obsługa mechanizmu split-tuneling).
2. Możliwość konfiguracji numeru portu, na którym działa usługa SSL VPN.
3. Klient VPN musi być dostępny dla następujących rodzajów systemów operacyjnych:
4. Microsoft Windows
5. Apple MacOS
6. Android
7. Linux
8. Urządzenie musi umożliwić realizację klienckich połączeń VPN dla urządzeń mobilnych pracujących w oparciu o systemy dla Apple (w tym IOS i iPadOS).

~~Ilość zdalnych połączeń VPN nie może być ograniczona.~~

# Redundancja, monitoring i wykrywanie awarii

1. Możliwość łączenia w klaster Active-Active lub Active-Passive (w obu trybach powinna istnieć funkcja synchronizacji sesji).
2. Możliwość wyboru interfejsów fizycznych w oparciu, o które realizowane będą funkcje weryfikacji działania klastra oraz funkcje synchronizacji sesji w obrębie klastra.
3. Wykrywanie awarii i uszkodzeń elementów sprzętowych
4. Monitoring łącz sieciowych oraz zdarzeń związanych z bezpieczeństwem sieci.

# Wymagania dla połączeń Site to Site VPN (parametry IPsec)

1. Wsparcie dla IKE v1 oraz v2
2. Obsługę szyfrowania protokołem AES z kluczem 256 bitów, lub dłuższym
3. Obsługę protokołu Diffie-Hellman grup 14 i wyżej
4. Obsługę SHA256.
5. Wsparcie dla pracy w topologii Hub and Spoke oraz Full Mesh.
6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
7. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth

# Szczegółowe wymagania fizyczne oraz wydajnościowe NGFW

Szczegółowe wymagania funkcjonalne i wydajnościowe urządzeń, które mają spełniać dostarczane urządzenia zestawiono w poniższych Tabelach:

Tabela nr 1 - Urządzenia NGFW wysokiej wydajności 1 sztuka

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Wymagany parametr** | **Wartość** |
| **1.** | Przepustowość (Throughput) wyznaczona jako wartość w [bps]. Uruchomione filtrowanie pakietów tylko do warstwy 4 modelu OSI [[1]](#footnote-2) | co najmniej 78 Gbps |
| **~~2.~~** | ~~Przepustowość (Throughput) z mechanizmami~~**~~Firewall, IPS, Application Control, Malware~~****~~Protection~~** ~~wyznaczona jako wartość w [bps] 2.~~ | ~~co najmniej 5.2Gbps~~ |
| **2.A** | Przepustowość **NGFW/NGIPS Throughput**wyznaczona jako wartość w [bps] [[2]](#footnote-3). | co najmniej 5.2 Gbps |
| **2.B** | Przepustowość **Threat Prevention Throughput** wyznaczona jako wartość w [bps]. | co najmniej 2,9 Gbps |
| **3.** | Inspekcja ruchu szyfrowanego TLS1.2 [[3]](#footnote-4) | co najmniej 1.5Gbps |
| **4.** | Inspekcja jednoczesnych połączeń HTTP | co najmniej 300 000 |
| **5.** | Ilość jednoczesnych połączeń | co najmniej 17 milionów |
| **6.** | Ilość nowych sesji TCP na sekundę | 350 000 |
| **7.** | Minimalna ilość reguł/polityk bezpieczeństwa (**Firewall Policies**), które mogą zostać utworzone na urządzeniu przy zachowaniu wymaganych parametrów wydajnościowych | 1000 |
| **8.** | Minimalna przepustowość tuneli VPN (**IPsec VPN Throughput**), opartych protokół IPsec dla AES256 oraz SHA256, wyznaczona jako wartość w [bps]. | 21 Gbps |
| **9.** | Ilość jednoczesnych tuneli IPsec w trybie Gateway-to-Gateway. | 90 000 |
| **10.** | Ilość jednoczesnych tuneli IPsec w trybie Remote Access | nielimitowane |
| **11.** | Minimalna ilość portów 1Gbps RJ45 | 8 |
| **12.** | Minimalna ilość portów 10 Gbps Ethernet SFP+ | 4 |
| **14.** | Ilość zasilaczy [[4]](#footnote-5) | 2 |
| **15.** | Ilość miejsca w szafie rack 19” | 1U |
| **16.** | Minimalny zakres wymaganych dodatkowych licencji i subskrypcji:* IPS – Intrusion Prevention System
* Application Control
* SSL Decryption/Inspection
* Malware Protection

- Forcepoint NGFW Management Center [[5]](#footnote-6) | [Tak] |

Tabela nr 2 - Urządzenia NGFW średniej wydajności 10 sztuk w tym jedno urządzenie zapasowe

|  |  |  |
| --- | --- | --- |
| **L.p.**  | **Wymagany parametr** | **Wartość**  |
| **1.**  | Przepustowość (Throughput) (uruchomione filtrowanie pakietów tylko do warstwy 4 modelu OSI [[6]](#footnote-7) | co najmniej 38 Gbps  |
| **~~2.~~** | ~~Przepustowość (Throughput) z mechanizmami~~**~~Firewall, IPS, Application Control, Malware~~** **~~Protection~~** ~~wyznaczona jako wartość w [bps] 2.~~ | ~~co najmniej 1.8Gbps~~ |
| **2.A** | Przepustowość **NGFW/NGIPS Throughput**wyznaczona jako wartość w [bps] [[7]](#footnote-8). | co najmniej 1,8 Gbps |
| **2.B** | Przepustowość **Threat Prevention Throughput** wyznaczona jako wartość w [bps]. | co najmniej 1,4 Gbps |
| **3.** | Inspekcja ruchu szyfrowanego TLS1.2 [[8]](#footnote-9) | co najmniej 690 Mbps |
| **4.** | Inspekcja jednoczesnych połączeń HTTP | co najmniej 70 000 |
| **5.** | Ilość jednoczesnych połączeń | co najmniej 5 milionów |
| **6.**  | Ilość nowych sesji TCP na sekundę  | 160 000  |
| **7.**  | Minimalna ilość reguł/polityk bezpieczeństwa (**Firewall Policies**), które mogą zostać utworzone na urządzeniu przy zachowaniu wymaganych parametrów wydajnościowych | 1000 |
| **8.**  | Minimalna przepustowość tuneli VPN (**IPsec VPN Throughput**), opartych protokół IPsec dla AES256 oraz SHA256, wyznaczona jako wartość w [bps].  |  10 Gbps  |
| **9.**  | Minimalna ilość jednoczesnych tuneli IPsec w trybie Gateway-to-Gateway.  | 20 000  |
| **10.**  | Ilość jednoczesnych tuneli IPsec w trybie Remote Access | nielimitowane |
| **11.**  | Minimalna ilość portów 1Gbps RJ45  |  8 |
| **12.** | Minimalna ilość portów 10 Gbps Ethernet SFP+ | 4 |
| **13.** | Port 2.5 Gbps Ethernet RJ45 | 1 |
| **14.**  | Ilość zasilaczy [[9]](#footnote-10)  | 2 |
| **15.** | Ilość miejsca w szafie rack 19”  | 1U  |
| **16.**  | Minimalny zakres wymaganych dodatkowych licencji i subskrypcji[[10]](#footnote-11): * IPS – Intrusion Prevention System
* Application Control
* SSL Decryption/Inspection
* Malware Protection

- Forcepoint NGFW Management Center [[11]](#footnote-12) | [Tak] |

Tabela nr 3 - Urządzenia NGFW niskiej wydajności 7 sztuk w tym jedno urządzenie zapasowe

|  |  |  |
| --- | --- | --- |
| **L.p.**  | **Wymagany parametr** | **Wartość**  |
| **1.**  | Przepustowość (Throughput) wyznaczona jako wartość w [bps]. Uruchomione filtrowanie pakietów tylko do warstwy 4 modelu OSI [[12]](#footnote-13) | co najmniej 3.8 Gbps  |
| **~~2.~~** | ~~Przepustowość (Throughput) z mechanizmami~~**~~Firewall, IPS, Application Control, Malware~~** **~~Protection~~** ~~wyznaczona jako wartość w [bps] 2~~ | ~~co najmniej 440 Mbps~~ |
| 2 | Przepustowość **NGFW/NGIPS Throughput**wyznaczona jako wartość w [bps] [[13]](#footnote-14). | co najmniej 440 Mbps |
| **3.** | Inspekcja ruchu szyfrowanego TLS1.2 [[14]](#footnote-15) | co najmniej 120 Mbps |
| **4.** | Inspekcja jednoczesnych połączeń HTTP | co najmniej 40 000 |
| **5.** | Ilość jednoczesnych połączeń | co najmniej 3,2 miliona |
| **6.**  | Ilość nowych sesji TCP na sekundę  | 48 000  |
| **7.**  | Minimalna ilość reguł/polityk bezpieczeństwa (**Firewall Policies**), które mogą zostać utworzone na urządzeniu przy zachowaniu wymaganych parametrów wydajnościowych |  1000  |
| **8.**  | Minimalna przepustowość tuneli VPN (**IPsec VPN Throughput**), opartych protokół IPsec dla AES256 oraz SHA256, wyznaczona jako wartość w [bps].  |  1.8 Gbps  |
| **9.**  | Ilość jednoczesnych tuneli IPsec w trybie Gateway-to-Gateway.  | 18 000  |
| **10.**  | Minimalna ilość jednoczesnych tuneli IPsec w trybie Remote Access | Nielimitowanerównoległa ilość tuneli IPSec w trybie Remote Access wynosi 25 |
| **11.**  | Minimalna ilość portów 1Gbps RJ45  |  8 |
| **12.**  | Minimalny zakres wymaganych dodatkowych licencji i subskrypcji[[15]](#footnote-16): * IPS – Intrusion Prevention System
* Application Control
* SSL Decryption/Inspection
* Malware Protection

- Forcepoint NGFW Management Center [[16]](#footnote-17) | [Tak] |

Tabela nr 4 – Wkładki światłowodowe kompatybilne z dostarczanymi urządzeniami (NGFW):

|  |  |  |  |
| --- | --- | --- | --- |
| Rodzaj wkładki | SFP 1Gb MM | SFP+ 10Gb SM | SFP+ 10Gb MM |
| Wymagania | Oryginalne wkładki producenta dostarczanych urządzeń |
| Liczba wkładek | 7 | 8 | 4 |

# Zgodność urządzeń z Centralnym Systemem Zarządzania (CSZ)

Dostarczane urządzenia muszą być zgodne z Centralnym Systemem Zarządzania zamawiającego, którym jest Forcepoint NGFW Security Management Center:

1. Dostarczane urządzenia NGFW muszą być zarządzane przez Centralny System Zarządzania (Forcepoint SMC)
2. Komunikacja pomiędzy zarządzanymi urządzeniami NGFW a Centralnym Systemem Zarządzania musi być szyfrowana
3. Komunikacja z serwerem zarządzającym musi odbywać się za pomocą:
* Interfejsu wiersza poleceń (ang. Command Line Interface, CLI) poprzez SSH
* Interfejs graficzny, poprzez przeglądarkę internetową (ang. web browser)
* Klienta – dedykowanego oprogramowania dostarczonego przez producenta rozwiązania
* Interfejs programistyczny (API).
1. Centralny System Zarządzania musi umożliwiać dostęp wielu Administratorom w tym samym czasie do konsoli zarządzającej oraz pozwalać na jednoczesny zapis elementów konfiguracji wraz z rozwiązywaniem konfliktów dostępu. W szczególności niedopuszczalna jest sytuacja, w której dwóch administratorów będzie modyfikowało w tym samym czasie ten sam obiekt (przykładowo politykę).
2. Centralny System Zarządzania musi umożliwiać zarządzanie wersjami konfiguracji wykorzystujące co najmniej wymienione poniżej funkcje:
* Praca na urządzeniu NGFW odbywa się na bazie konfiguracji kandydackiej, a nie aktywnej.
* Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu NGFW jest możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej.
* CSZ posiada narzędzie walidacji polityki umożliwiające wskazanie nieosiągalnych reguł, zduplikowanych lub innych możliwych problemów wynikających z błędów konfiguracji
* Możliwość przywrócenia konfiguracji z określnego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, liczba przechowywanych w ten sposób konfiguracji nie może być mniejsza niż 50, podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.
1. Rozwiązanie musi umożliwić realizację dostępu do konsoli zarządzającej z wykorzystaniem certyfikatów użytkowników dostępnych na nośnikach przenośnych (przykładowo USB)
2. System zarządzania umożliwia uwierzytelnianie użytkowników administracyjnych za pomocą:
* Bazy lokalnej
* Serwera RADIUS
* Serwera TACACS+
1. CSZ zapewnia przydział uprawnień administratorom z podziałem na role administracyjne (RBAC), w tym minimalnie:
* Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu
* Operator, który ma możliwość tylko odczytu konfiguracji.
1. System zapewnia logi typu Audit z pełną informacją o czynnościach podjętych przez Administratorów
2. System musi umożliwiać gromadzenie i przechowywanie logów zdarzeń
3. System musi posiadać wbudowany mechanizm raportowania bez konieczności stosowania dodatkowych licencji. Mechanizm ten umożliwia przeglądanie raportów ze zdarzeń w czasie rzeczywistym. Przestrzeń do przechowywania logów nie jest ograniczona licencyjnie
4. System musi posiadać mechanizm filtrowania, przeszukiwania i korelacji logów zdarzeń
5. System musi posiadać funkcjonalność powiadamiania administratorów o zdarzeniach za pomocą e-mail.
6. Logi w systemie powinny zawierać następujące informację:
* adres źródłowy i docelowy w formacie FQDN lub IP, port źródłowy i docelowy, wykorzystywaną aplikację sieciową oraz protokół
* informację o użytkowniku, który realizował dane połączenie sieciowe
* znacznik czasu (minimum data, godzina, sekunda)
* przypisanie zdarzenia do polityki odpowiadającej za jego wygenerowanie -informacja o rodzaju zdarzenia (przykładowo atak typu: DoS, malware, exploit, skanowanie)

# Współpraca nowych urządzeń NGFW z posiadanymi obecnie przez Zamawiającego

Dostarczane urządzenia muszą umożliwiać tworzenie klastrów wydajnościowych oraz niezawodnościowych z obecnie posiadanymi urządzeniami:

* Dostarczane urządzenia NGFW średniej wydajności muszą współpracować w klastrze w trybie active-active i active-passive z urządzeniami N335 oraz N2101
* Dostarczane urządzenia NGFW wysokiej wydajności muszą współpracować w klastrze w trybie active-active i active-passive z urządzeniami N2101
* Dołączenie nowych urządzeń do pracy w klastrze z posiadanymi urządzeniami nie może wymagać dokupienia żadnych dodatkowych licencji lub subskrypcji do posiadanych urządzeń, a także nie może naruszać warunków wsparcia technicznego dla posiadanych urządzeń

# Dokumentacja przedwdrożeniowa

1. Wykonawca przedstawi Zamawiającemu dokumentację przedwdrożeniową w postaci szczegółowego harmonogramu prac oraz ich zakresu.
2. Przed przystąpieniem do prac instalacyjnych Zamawiający przedstawi wytyczne do konfiguracji wstępnej instalowanych urządzeń a Wykonawca zaproponuje i uzgodni z Zamawiającym konfigurację wstępną. Podstawowym założeniem dla konfiguracji wstępnej urządzenia jest jego podłączenie i skomunikowanie z Centralnym Systemem Zarządzania, aby umożliwić dalszą zdalną konfigurację urządzenia Zamawiającemu.
3. Wykonawca przystąpi do prac instalacyjnych po zaakceptowaniu przez Zamawiającego dokumentacji przedwdrożeniowej.

# Wymagania dotyczące instalacji dodatkowych urządzeń w sieci WAN Zamawiającego

1. Wykonawca dostarczy, skonfiguruje, zainstaluje i uruchomi nowe urządzenia w lokalizacjach placówek Sieci Badawczej Łukasiewicz wskazanych przez Zamawiającego znajdujących się na terenie Rzeczpospolitej Polskiej. Prace zostaną wykonane zgodnie z zaakceptowaną dokumentacją przedwdrożeniową oraz uzgodnionymi ustaleniami operacyjnymi.
2. Wykonawca dokona aktywacji licencji wymaganych do uruchomienia funkcjonalności wszystkich nowych urządzeń i przyłączenia ich do Centralnego Systemu Zarządzania.
3. Wykonawca skonfiguruje nowe urządzenia w celu umożliwienia Zamawiającemu objęcia nowych urządzeń Centralnym Systemem Zarządzania.
4. Wymagane jest wykonanie aktualizacji oprogramowania do najnowszej (rekomendowanej przez producenta) wersji.
5. W przypadku konieczności wykonania instalacji w siedzibie Zamawiającego, prace będą wykonywane pod nadzorem pracowników Zamawiającego.
6. Prace będą wykonywane w taki sposób, aby nie powodować przerw w działaniu infrastruktury sieciowej Zamawiającego oraz godzinach uzgodnionych z daną lokalizacją przez Zamawiającego (Zamawiający dopuszcza pracę zdalną).
7. W przypadku prac, które mogą mieć wpływ na ciągłość działania infrastruktury sieciowej Zamawiającego będą wykonywane w określonych, uzgodnionych z Zamawiającym godzinach poza godzinami pracy.
8. Po zakończonych pracach instalacyjnych Wykonawca przygotuje zestawienie wykonanych zmian i konfiguracji do dołączenia do dokumentacji powdrożeniowej.
9. Zamawiający wymaga, aby przynajmniej jedna osoba wykonująca prace konfiguracji i uruchomienia posiadała certyfikaty z zakresu technologii wdrażanych w ramach usługi, autoryzowane przez producenta dostarczonych urządzeń, na poziomie zaawansowanym (certyfikat na poziomie professional lub inny odpowiadający poziomowi professional, czyli poziom przynajmniej o jeden wyższy niż poziom podstawowy certyfikatu).
10. Wszystkie narzędzia i części montażowe niezbędne do instalacji uruchomienia urządzeń i sieci WAN zapewnia Wykonawca.
11. Wykonanie dostaw oraz prac instalacyjnych, zgodnie z wymaganiami, zostanie potwierdzone obustronnie podpisanym protokołem wykonania.
12. Do zadań Wykonawcy nie należy:
	1. Modernizacja sieci LAN zamawiającego.
	2. Migracja istniejących polityk bezpieczeństwa na urządzeniach posiadanych obecnie przez zamawiającego

# Wymagania dotyczące gwarancji (usuwanie awarii)

1. Zamawiający wymaga udzielenia gwarancji na nowe urządzenia na okres 36 miesięcy.
2. Urządzenia muszą mieć zapewnione wsparcie techniczne w okresie gwarancji, w szczególności dostęp do aktualizacji oprogramowania firmowego producenta urządzeń
3. Wykonawca zapewni jeden punkt kontaktowy do przyjmowania wszystkich zgłoszeń. Zgłoszenia mogą być kierowane za pomocą następujących kanałów: strona www, email, telefon.
4. Wykonawca zapewni przyjmowanie zgłoszeń awarii lub problemu technicznego przez 7 dni w tygodniu, 24 godziny na dobę.
5. Czas reakcji – do 4 godzin (Przez czas reakcji rozumie się potwierdzenie przyjęcia zgłoszenia i podjęcie działań zmierzających do usunięcia awarii).
6. Gwarantowany czas usunięcia awarii - pierwszy dzień roboczy po dniu w którym nastąpiło zgłoszenie awarii.
7. Przez usunięcie awarii rozumie się przywrócenie funkcjonalności sprzed awarii. W przypadku awarii softwarowych dopuszcza się zastosowanie rozwiązania tymczasowego (tzw. workaround) do czasu wprowadzenia rozwiązania docelowego, jednak nie dłużej niż 90 dni kalendarzowych.
8. W przypadku niemożności naprawy sprzętu w terminie określonym w pkt 6, Wykonawca zapewni Zamawiającemu sprzęt zastępczy (tego samego producenta), o parametrach nie gorszych niż naprawiany sprzęt do czasu naprawy uszkodzonego sprzętu (przez naprawę urządzenia rozumie się naprawę urządzenia przywracającą funkcjonalność sprzed awarii lub wymianę na nowe urządzenie tego samego typu).
9. W przypadku wymiany uszkodzonego urządzenia na nowe, urządzenie wymienione musi posiadać wszystkie wymagane cechy, być całkowicie sprawne, objęte serwisem i gwarancją na tych samych zasadach.

# Wymagania dotyczące wsparcia powdrożeniowego

Wykonawca zobowiązany jest do zapewnienia wsparcia powdrożeniowego w ramach puli o  wymiarze 150 roboczogodzin w okresie 12 miesięcy od dnia podpisania protokołu odbioru. Zakres i harmonogram prac powdrożeniowych będzie przekazywany przez Zamawiającego i uzgadniany na bieżąco z Wykonawcą. Do wykonania prac powdrożeniowych Wykonawca skieruje wykwalifikowany personel posiadający wiedzę pozwalającą na uzyskanie certyfikatu producenta urządzeń na poziomie professional. Rozliczenie wsparcia powdrożeniowego zostanie dokonane według stałej ceny jednostkowej roboczogodziny i faktycznej realizacji roboczogodzin, rozliczane po zakończeniu każdego kwartału. Zamawiający nie ma obowiązku wykorzystania całej puli roboczogodzin.

1. UDP 1518 byte [↑](#footnote-ref-2)
2. HTTP 64kB (payload) [↑](#footnote-ref-3)
3. HTTP 44kB (payload) [↑](#footnote-ref-4)
4. NGFW ma zostać dostarczone z wymaganą liczbą zasilaczy. [↑](#footnote-ref-5)
5. Licencje umożliwiające objęcie nowych urządzeń Centralnym Systemem Zarządzania, wymaga się zapewnienia subskrypcji co najmniej do dnia 14.04.2025 [↑](#footnote-ref-6)
6. UDP 1518 byte [↑](#footnote-ref-7)
7. HTTP 64kB (payload) [↑](#footnote-ref-8)
8. HTTP 44kB (payload) [↑](#footnote-ref-9)
9. NGFW ma zostać dostarczone z wymaganą liczbą zasilaczy. [↑](#footnote-ref-10)
10. Dla urządzeń zapasowych nie wymaga się dostarczenia licencji oraz subskrypcji [↑](#footnote-ref-11)
11. Licencje umożliwiające objęcie nowych urządzeń Centralnym Systemem Zarządzania, wymaga się zapewnienia subskrypcji co najmniej do dnia 14.04.2025 [↑](#footnote-ref-12)
12. UDP 1518 byte [↑](#footnote-ref-13)
13. HTTP 64kB (payload) [↑](#footnote-ref-14)
14. HTTP 44kB (payload) [↑](#footnote-ref-15)
15. Dla urządzeń zapasowych nie wymaga się dostarczenia licencji oraz subskrypcji [↑](#footnote-ref-16)
16. Licencje umożliwiające objęcie nowych urządzeń Centralnym Systemem Zarządzania, wymaga się zapewnienia subskrypcji co najmniej do dnia 14.04.2025 [↑](#footnote-ref-17)