BF-IV.2370.12.2024
Warszawa, 08-10-2024 r.

Uczestnicy postępowania

Dotyczy: modyfikacji OPZ w postępowaniu przetargowym na „Dostawę urządzeń infrastruktury sieci SD-WAN dla platformy chmurowej integracji danych Komendy Głównej Państwowej Straży Pożarnej".

Zamawiający dokonuje zmiany w treści Załącznika nr 1 stanowiącego OPZ w następującym zakresie:

1. Dotychczasowy zapis OPZ:
„Wstęp
Celem tego zamówienia jest stworzenie na bazie dostarczonych urządzeń, spójnego i zintegrowanego systemu komunikacyjnego, który umożliwi efektywny, szybki i bezpieczny przepływ krytycznych informacji w ramach działań Państwowej Straży Pożarnej i innych służb odpowiedzialnych za bezpieczeństwo publiczne. Przedmiotowe zadanie obejmuje dostawę i wyposażenie 553 lokalizacji PSP w urządzenia w ilości 605 sieci SD-WAN w celu stworzenia zaawansowanego i zintegrowanego systemu komunikacyjnego opartego na technologii SDWAN."

Otrzymuje następujące brzmienie:
„Wstęp
Celem tego zamówienia jest stworzenie na bazie dostarczonych urządzeń spójnego i zintegrowanego systemu komunikacyjnego, który umożliwi efektywny, szybki i bezpieczny przepływ krytycznych informacji w ramach działań Państwowej Straży Pożarnej (PSP) oraz innych służb odpowiedzialnych za bezpieczeństwo publiczne. Przedmiotowe zadanie obejmuje dostawę i wyposażenie 550 lokalizacji PSP w urządzenia, w ilości 605 sieci SD-WAN, w celu stworzenia zaawansowanego i zintegrowanego systemu komunikacyjnego opartego na technologii SD-WAN (Software-Defined Wide Area Network).
Zadanie to jest częścią projektu rozbudowy Platformy Chmurowej Integracji Danych KG PSP (PCID-KGPSP), który realizowany jest w ramach projektu SOIA (System Ostrzegania i Alarmowania Ludności). Technologia SD-WAN zapewni wydajną i bezpieczną komunikację między jednostkami PSP i OSP, integrując ponad 4000 urządzeń ostrzegania oraz pojazdy dowodzenia i łączności, co przyczyni się do poprawy działania systemów ostrzegania i 2 alarmowania. SD-WAN umożliwi centralne zarządzanie siecią, co jest kluczowe dla sprawnego funkcjonowania działań ratowniczych w skali całego kraju.

ul. Podchorążych 38
00-463 Warszawa
www.gov.pl/web/kgpsp

Projekt ten jest dla nas szczególnie istotny ze względu na uwarunkowania w zakresie cyberbezpieczeństwa. Wymóg ten wynika z konieczności zapewnienia odpowiedniego poziomu bezpieczeństwa, którego kryteria zostały określone przez Zamawiającego w oparciu o postanowienia Uchwały Nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy "Wspólna Infrastruktura Informatyczna Państwa". Projekt uwzględnia Narodowe Standardy Cyberbezpieczeństwa oraz Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO). Zgodność z tymi przepisami jest również wymogiem Ustawy o krajowym systemie cyberbezpieczeństwa, która obliguje podmioty publiczne do zapewnienia ochrony systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych. Zamawiający, jako podmiot publiczny, jest odpowiedzialny za stosowanie standardów cyberbezpieczeństwa, które zapewniają wysoki poziom ochrony systemów teleinformatycznych PSP. W szczególności, lokalizacja urządzeń typu sandbox na terenie Polski jest wymagana w celu minimalizacji ryzyka oraz zapewnienia maksymalnej kontroli nad przetwarzanymi danymi, zgodnie z analizą potrzeb i obowiązującymi przepisami, takimi jak Ustawa o krajowym systemie cyberbezpieczeństwa, Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz Narodowe Standardy Cyberbezpieczeństwa.

2. Dotychczasowy zapis OPZ:
„Opis stanu obecnego.
Obecnie wszystkie jednostki PSP mają dostęp do sieci OST112 oraz sieci operatorów ISP z dostępem do Internetu. Zabezpieczenia ruchu sieciowego są zdecentralizowane i nie mają ustandaryzowanej konfiguracji zabezpieczeń sieci, nie są agregowane logi w kontekście całej organizacji i jej bezpieczeństwa. W powyższej konfiguracji nie jest możliwe zorganizowanie implementacji wspólnej polityki dostępu, zabezpieczeń sieci i jej automatycznej analizy dla realizacji szybkiej reakcji na potencjalne ataki z zewnątrz itp.
Ruch sieciowy wewnątrz organizacji do systemów centralnych i pomiędzy jednostkami odbywa się poprzez sieć OST 112. Nie jest wykorzystywana sieć dostępu do Internetu jako zapasowe łącze.

Próby organizacji zapasowych połączeń wykorzystujących jako medium transmisyjne sieć Internet były wdrażane na poziomach Komend Wojewódzkich PSP w relacji połączenia z podległymi Komendami, co w korelacji dostępu do usług centralnych nie stanowi poprawy dostępności dodatkowego kanału połączeniowego wdrażanego lokalnie.
Urządzenia zabezpieczające dostęp do sieci Internet mają różny poziom implementacji rozwiązań bezpieczeństwa i są kupowane przez każdą Jednostkę

Organizacyjną z osobna, co stanowi bardzo duże koszty utrzymania poziomu zabezpieczeń.
W dotychczasowych połączeniach z siecią OST 112 brak jest mechanizmów ukierunkowanych na usługę, aplikacje i ich dostępność, co skutkuje losowym poziomem jakości dostępu. Zamawiający dysponuje urządzeniami brzegowymi w siedzibie KG PSP oraz personel posiadający certyfikowane szkolenia oraz doświadczenie w zakresie zarządzania konfiguracji NG firewall."

Otrzymuje następujące brzmienie:
„**Opis stanu obecnego**.
Obecnie wszystkie jednostki PSP posiadają dostęp do sieci OST112 oraz sieci operatorów ISP, jednak zabezpieczenia ruchu sieciowego są zdecentralizowane, co prowadzi do braku spójnej polityki bezpieczeństwa. Nie ma ustandaryzowanej konfiguracji zabezpieczeń, a logowanie zdarzeń nie jest agregowane na poziomie całej organizacji, co uniemożliwia centralną analizę i szybkie reagowanie na zagrożenia. Ruch sieciowy wewnątrz organizacji odbywa się wyłącznie przez sieć OST112, bez wykorzystania łącza internetowego jako zapasowego.
Urządzenia zabezpieczające dostęp do Internetu są kupowane i zarządzane indywidualnie przez każdą jednostkę, co generuje wysokie koszty utrzymania i różne poziomy zabezpieczeń. Brakuje mechanizmów optymalizujących dostępność usług i aplikacji, co skutkuje zmienną jakością połączeń. Komenda Główna PSP posiada urządzenia NG Firewall oraz personel z certyfikowanymi umiejętnościami ich zarządzania, ale cała infrastruktura wymaga centralizacji i standaryzacji."

3. Dotychczasowy zapis OPZ:

„Główne cele:
- Umożliwienie efektywnego współdziałania różnorodnych systemów i technologii używanych przez Państwową Straż Pożarną oraz inne służby ratunkowe, co umożliwi szybką i skoordynowaną reakcję w sytuacjach kryzysowych,
- Zapewnienie odporności rozwiązania na różnego rodzaju awarie i zagrożenia, co jest kluczowe dla utrzymania ciągłości komunikacji w trakcie działań ratunkowych i sytuacji kryzysowych,
- Wymiana danych musi spełniać najwyższe standardy bezpieczeństwa, aby zapobiegać nieautoryzowanemu dostępowi i utracie ważnych informacji,
- Rozwiązanie musi być projektowane z myślą o łatwej rozbudowie i integracji nowych jednostek oraz użytkowników, co umożliwi elastyczne dostosowanie do zmieniających się potrzeb,
- Wszelkie działania i rozwiązania muszą być zgodne z obowiązującymi przepisami prawnymi dotyczącymi ochrony danych i bezpieczeństwa informacji,

- Stworzenie zaawansowanego nadzoru i kontroli nad polityką dostępu do zasobów sieci Internet i innych sieci,
- Wdrożenie centralnego systemu bezpieczeństwa przed potencjalnymi atakami z sieci Internet poprzez wprowadzenie centralnych punktów styku,
- Możliwość szybkiego reagowania administratorów IT na lokalne, bieżące potrzeby w zakresie polityki dostępu,
- Centralna archiwizacja konfiguracji i możliwość jej audytu przez administratorów Komendy Głównej PSP pod kątem zgodności z centralną polityką dostępu,
- Sieć SD-WAN przystosowana do obsługi i świadczenia usług na każdym poziomie wszystkich jednostek podległych w tym m.in. takich jak łączność wideo, voip, dostęp do zasobów chmury prywatnej, publicznej etc.
- Wizualizacja ruchu sieciowego i jego analiza dla zapewnienia wysokiej dostępności usług, aplikacji,
- połączenie wszystkich Podmiotów wymienionych w załączniku nr 2a do umowy (wykaz lokalizacji dostaw i instalacji urządzeń dla poszczególnych Odbiorców) poprzez sieć SD-WAN przy wykorzystaniu istniejącej infrastruktury technicznej i jej rozbudowa o kolejne moduły sprzętowe."

Otrzymuje następujące brzmienie:

„Główne cele:
1. Zapewnienie interoperacyjności systemów – Celem jest stworzenie rozwiązań umożliwiających sprawne współdziałanie różnych systemów i technologii wykorzystywanych przez Państwową Straż Pożarną oraz inne służby ratownicze. Poprzez integrację tych systemów, możliwe będzie szybsze i bardziej skoordynowane reagowanie w sytuacjach kryzysowych, co jest kluczowe dla skuteczności działań operacyjnych.
2. Odporność na awarie i zagrożenia – Kluczowym elementem jest zapewnienie wysokiej odporności infrastruktury sieciowej na różnego rodzaju awarie i zagrożenia zewnętrzne, co jest niezbędne do utrzymania ciągłości komunikacji i operacyjności systemów podczas działań ratowniczych.
3. Bezpieczeństwo danych – Wszystkie procesy wymiany danych muszą spełniać najwyższe standardy bezpieczeństwa, chroniąc przed nieautoryzowanym dostępem, atakami cybernetycznymi oraz utratą krytycznych informacji. Szczególny nacisk kładzie się na zgodność z przepisami dotyczącymi ochrony danych osobowych oraz bezpieczeństwa teleinformatycznego.
4. Elastyczność i skalowalność infrastruktury – Systemy muszą być projektowane z myślą o łatwej rozbudowie i integracji nowych jednostek operacyjnych oraz użytkowników.

Elastyczna architektura zapewni adaptację do zmieniających się wymagań operacyjnych i technologicznych, co pozwoli na szybkie wdrażanie nowych funkcji i usług.

5. Zgodność z regulacjami prawnymi – Wszelkie wdrażane rozwiązania muszą być zgodne z aktualnymi przepisami prawnymi dotyczącymi ochrony danych, bezpieczeństwa informacji oraz przepisami dotyczącymi działań ratowniczych, w tym z ustawą o ochronie przeciwpożarowej.

6. Zarządzanie dostępem do sieci i zasobów – Wdrożenie zaawansowanego systemu nadzoru nad polityką dostępu do sieci, który umożliwi precyzyjną kontrolę nad korzystaniem z zasobów sieciowych, takich jak internet oraz inne sieci wewnętrzne. Centralizacja polityki dostępu umożliwi administratorom sprawne zarządzanie i monitorowanie aktywności użytkowników.

7. Ochrona przed zagrożeniami z internetu – Kluczowe jest wdrożenie centralnych punktów styku sieci, które będą stanowiły ochronę przed zagrożeniami płynącymi z internetu, w tym atakami cybernetycznymi, z możliwością monitorowania i reagowania na potencjalne zagrożenia w czasie rzeczywistym.

8. Centralizacja zarządzania konfiguracją – Konfiguracje urządzeń sieciowych powinny być archiwizowane w sposób centralny, z możliwością audytów zgodności z przyjętą polityką bezpieczeństwa i dostępności przez administratorów KG PSP. Umożliwi to łatwe zarządzanie zmianami i weryfikację zgodności infrastruktury z wymogami operacyjnymi.

9. Wsparcie dla technologii SD-WAN – Sieć SD-WAN powinna być przystosowana do obsługi zróżnicowanych usług, takich jak wideokonferencje, VoIP, dostęp do zasobów chmurowych (zarówno prywatnych, jak i publicznych). Jej wdrożenie zapewni wysoką dostępność oraz wydajność dla wszystkich jednostek organizacyjnych podległych PSP, z uwzględnieniem potrzeb operacyjnych.

10. Analiza i wizualizacja ruchu sieciowego – System powinien umożliwiać zaawansowaną analizę ruchu sieciowego w celu identyfikacji potencjalnych problemów oraz zapewnienia optymalnej dostępności usług krytycznych, co jest kluczowe dla operacyjności jednostek ratowniczych.

11. Rozbudowa infrastruktury SD-WAN – Wdrażane rozwiązanie musi umożliwić połączenie wszystkich lokalizacji wymienionych w załączniku nr 2a, z wykorzystaniem istniejącej infrastruktury technicznej oraz jej rozbudowę o dodatkowe moduły sprzętowe, co zapewni skalowalność i przyszłościową gotowość sieci.”

4. Dotychczasowy zapis OPZ:
„**Wymagania stawiane sieci SD-WAN**:
- Wysoka dostępność i niezawodność połączeń,
- Zaawansowane mechanizmy zabezpieczeń tj. m.in. szyfrowanie, firewall, IDS/IPS,
- Możliwość centralnego zarządzania i monitorowania sieci,
- Kompatybilność z obecnymi systemami teleinformatycznymi KG PSP,
- Elastyczność w konfiguracji połączeń zależnie od aktualnych potrzeb operacyjnych,
- Projekt ten jest niezbędny dla zwiększenia efektywności operacyjnej i bezpieczeństwa w działaniach Państwowej Straży Pożarnej.

W ramach wskazanych Podmiotów (załącznik nr 2a) zakłada się budowę 3 poziomów węzłów komunikacyjnych:
- Centralnych (CWK), obsługiwanych przez urządzenia Typ nr 1,
- Pośrednich (PWK), obsługiwanych przez urządzenia Typ nr 2,
- Końcowych (KWK), obsługiwanych przez urządzenia Typ nr 4.

Przyjęty podział zakłada gradacje wymagań wydajnościowych i funkcjonalnych dla sprzętu i oprogramowania w zależności od ustalonego przydziału wynikającego z załącznika nr 4 do umowy (wykaz ilościowy urządzeń przeznaczonych dla poszczególnych Odbiorców). Zamawiający wymaga dostawy i wdrożenia sprzętu i oprogramowania spełniającego niżej wymienione wymagania techniczne. Oferent jest zobowiązany dołączyć do oferty niezbędne dane informacyjne, dane katalogowe (w j. polskim lub j. angielskim), z których będzie wynikać, że oferowane rozwiązanie jest zgodne z wymaganiami technicznymi (linki do stron materiałów publikowanych przez producentów sprzętu).
Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek europejski i musi być objęta serwisem oraz wsparciem przez okres minimum 60 miesięcy od daty dostawy.
Całość dostarczanego sprzętu musi być nowa i nieużywana we wcześniejszych projektach (nie dopuszcza się zastosowania urządzeń tzw. Refurbished).
Na cały okres wdrożenia ze strony Zamawiającego oraz Wykonawcy zostaną wyznaczone osoby, pełniące rolę Koordynatorów wdrożenia, odpowiedzialne za kontakty i ustalania pomiędzy Zamawiającym, a Wykonawcą. Dane kontaktowe przedstawicieli poszczególnych Odbiorców umowy- koordynatorów zostaną przekazane na etapie realizacji przedmiotu umowy.”

Otrzymuje następujące brzmienie:

„Wymagania stawiane sieci SD-WAN:

1. Wysoka dostępność i niezawodność połączeń – Sieć SD-WAN musi gwarantować nieprzerwaną i niezawodną komunikację między jednostkami PSP oraz centralnymi systemami, nawet w warunkach zwiększonego obciążenia sieciowego lub potencjalnych awarii.
2. Zaawansowane mechanizmy zabezpieczeń – System musi zapewniać kompleksową ochronę danych poprzez wdrożenie mechanizmów takich jak szyfrowanie połączeń, firewall nowej generacji (NGFW), oraz systemy wykrywania i zapobiegania włamaniom (IDS/IPS). Zabezpieczenia te mają kluczowe znaczenie dla ochrony sieci przed cyberzagrożeniami.
3. Możliwość centralnego zarządzania i monitorowania sieci – Sieć SD-WAN powinna umożliwiać scentralizowane zarządzanie politykami bezpieczeństwa, konfiguracjami urządzeń oraz monitorowanie w czasie rzeczywistym ruchu sieciowego i stanu infrastruktury. Wymaga się wdrożenia narzędzi umożliwiających administratorom sprawne zarządzanie wszystkimi lokalizacjami z jednego punktu kontrolnego.
4. Kompatybilność z obecnymi systemami teleinformatycznymi KG PSP – Nowa infrastruktura musi być w pełni zintegrowana z obecnymi systemami teleinformatycznymi Komendy Głównej PSP, zapewniając płynną współpracę z istniejącymi rozwiązaniami, aplikacjami i usługami. Ważna jest także kompatybilność z obecnie wdrożonymi technologiami, aby uniknąć problemów związanych z integracją.
5. Elastyczność w konfiguracji połączeń – Sieć musi być elastyczna, umożliwiając dynamiczne dostosowywanie połączeń sieciowych do zmieniających się potrzeb operacyjnych.

Możliwość automatycznego przełączania się między łączami (np. zapasowym łączem internetowym) w sytuacjach awaryjnych jest kluczowa dla zapewnienia ciągłości działań.

6. Zwiększenie efektywności operacyjnej i bezpieczeństwa – Wdrożenie tego projektu ma na celu podniesienie efektywności operacyjnej oraz poprawę poziomu bezpieczeństwa w działaniach Państwowej Straży Pożarnej. Rozwiązanie to będzie fundamentem infrastruktury teleinformatycznej, na której opierać się będą wszystkie kluczowe operacje PSP, w tym zarządzanie kryzysowe i komunikacja w sytuacjach awaryjnych.

W ramach projektu budowy sieci SD-WAN dla Państwowej Straży Pożarnej, planuje się implementację trzech poziomów węzłów komunikacyjnych, zróżnicowanych pod względem wydajności i funkcjonalności sprzętu oraz oprogramowania. Szczegóły te obejmują:

1. Węzły Centralne (CWK) – Będą one obsługiwane przez urządzenia Typ nr 1. Węzły centralne będą kluczowym elementem infrastruktury, odpowiadającym za zarządzanie i kontrolę ruchu sieciowego na poziomie całej sieci. Te urządzenia będą charakteryzowały się najwyższymi wymaganiami wydajnościowymi i funkcjonalnymi, odpowiednimi do obsługi centralnych systemów komunikacyjnych PSP.
2. Węzły Pośrednie (PWK) – Obsługiwane przez urządzenia Typ nr 2. Węzły te będą pełniły funkcję pośredników między węzłami centralnymi a końcowymi, zapewniając ciągłość przepływu danych oraz odpowiednią redundancję. Urządzenia Typ nr 2 będą dostosowane do realizacji zadań o średnich wymaganiach w zakresie wydajności i funkcjonalności.
3. Węzły Końcowe (KWK) – Obsługiwane przez urządzenia Typ nr 4. Węzły te będą instalowane na końcowych punktach komunikacyjnych, takich jak lokalne jednostki PSP. Urządzenia Typ nr 4 będą charakteryzowały się odpowiednią funkcjonalnością do obsługi lokalnych połączeń, gwarantując bezpieczną i wydajną transmisję danych na poziomie lokalnym.
Gradacja wymagań wydajnościowych i funkcjonalnych dla sprzętu i oprogramowania została określona na podstawie przydziałów wynikających z załącznika nr 4 do umowy (wykaz ilościowy urządzeń dla poszczególnych Odbiorców). Oferent ma obowiązek dostarczenia sprzętu oraz oprogramowania, które spełnia następujące wymagania techniczne:
• Dane informacyjne i katalogowe: Wykonawca zobowiązany jest dołączyć do oferty szczegółowe dane techniczne oferowanych urządzeń, potwierdzające ich zgodność z wymaganiami Zamawiającego. Dane te mogą być w języku polskim lub angielskim, a informacje o zgodności powinny być poparte materiałami publikowanymi przez producentów sprzętu (linki do stron producentów).
• Autoryzacja i serwis: Wszystkie dostarczone urządzenia oraz oprogramowanie muszą pochodzić z autoryzowanego kanału sprzedaży producentów na rynek europejski. Ponadto, muszą być objęte serwisem i wsparciem technicznym przez okres minimum 60 miesięcy od daty dostawy.
• Nowość i nieużywalność sprzętu: Zamawiający wymaga, aby cały dostarczony sprzęt był fabrycznie nowy, nieużywany w innych projektach. Sprzęt „Refurbished” (odnowiony) nie będzie akceptowany.
Wdrożenie projektu będzie nadzorowane przez wyznaczonych koordynatorów zarówno ze strony Zamawiającego, jak i Wykonawcy. Ich zadaniem będzie zarządzanie procesem wdrożenia, zapewnienie odpowiedniej komunikacji między stronami oraz ustalanie kluczowych kwestii na każdym etapie realizacji projektu. Dane kontaktowe koordynatorów ze strony Odbiorców zostaną przekazane na etapie realizacji umowy.”

5. Dotychczasowy zapis OPZ:
„Zakres zamówienia obejmuje:
- Implementację ogólnokrajowej sieci SD-WAN,
- Dostarczenie niezbędnego sprzętu i oprogramowania na poziomie Komendy Głównej PSP, komend wojewódzkich PSP, komend powiatowych/miejskich PSP w tym JRG oraz posterunków JRG, jak również szkół PSP i ośrodków szkolenia PSP,
- Integrację z istniejącą infrastrukturą IT PSP,
- Zapewnienie wsparcia technicznego i serwisu.

Dostarczone urządzenia muszą być w pełni kompatybilne z urządzeniami Zamawiającego, w tym z systemem zarządzania, tak aby można było zaimplementować polityki bezpieczeństwa oraz konfigurację polityk routingu na dostarczone urządzenia bez konieczności ich modyfikacji.
Kompatybilność musi obejmować obszary, takie jak:
- kompatybilność sprzętowa: zgodność na poziomie fizycznym, w tym złącza, interfejsy i protokoły komunikacyjne.
- kompatybilność programowa: zgodność z systemami operacyjnymi, oprogramowaniem zarządzającym oraz politykami bezpieczeństwa.
- kompatybilność operacyjna: możliwość implementacji polityk bezpieczeństwa i routingu bez konieczności modyfikacji dostarczonych urządzeń.

W przypadku dostawy rozwiązania innego niż funkcjonujące u Zamawiającego, Wykonawca dodatkowo, na własny koszt, dostarczy, skonfiguruje i wdroży równoważne rozwiązanie oparte na urządzeniach pracujących jako para wysokiej dostępności (HA) w trybach Active/Standby i Active/Active, wyposażone w system centralnego zarządzania i monitorowania NG Firewall.
Rozwiązanie to musi obejmować:
- odpowiednią ilość licencji i oprogramowania, przeniesienie i implementację wszystkich polityk i konfiguracji z pełnym odwzorowaniem funkcjonalności i bezpieczeństwa,
- zapewnić serwis gwarancyjny oraz wsparcie na okres co najmniej 60 miesięcy,
- zapewnić pełne wsparcie techniczne przez okres 60 miesięcy w trybie 24/7/365 z czasem reakcji do 2 godzin od zgłoszenia oraz maksymalnie 6 godzin na usunięcie awarii dla całego dostarczonego rozwiązania opisanego w niniejszym postępowaniu, - zapewnić certyfikowane szkolenia dla personelu Zamawiającego wraz ze wsparciem technicznym opisanym poniżej z uwagi na doświadczenie i samodzielne utrzymanie systemu przez personel Zamawiającego.

Rozwiązanie funkcjonujące u Zamawiającego zawiera m.in.:
- klaster dwóch urządzeń firewall nowej generacji Palo Alto PA 1420 wraz z pakietem subskrypcji Core Security: zaawansowane zapobieganie zagrożeniom, zaawansowane filtrowanie adresów URL, zaawansowany Wildfire,

zabezpieczenia DNS i SD-WAN (PAN-PA-1420-BND-CORESEC-5YR) na okres 60 miesięcy,
- wsparcie premium (PAN-SVC-BKLN-1420-5YR) na okres 60 miesięcy,
- oprogramowanie do centralnego zarządzania Panorama dla 100 urządzeń (PAN-PRA-100) ze wsparciem na okres 60 miesięcy,
- licencje na wirtualne systemy (10 szt.) dla 2 urządzeń,
- subskrypcje GlobalProtect z funkcją HIP (dla 2000 urządzeń końcowych) dla 2 urządzeń Palo Alto PA- 1420 pracujących w klastrze HA na okres 60 miesięcy.

Zamówienie obejmuje dostawę urządzeń infrastruktury sieci SD-WAN zgodnie z poniższą specyfikacją. W przypadku wskazania znaków towarowych, patentów lub pochodzenia, Zamawiający dopuszcza składanie ofert równoważnych, pod warunkiem że oferowane urządzenia spełniają minimalne wymagania określone w opisie przedmiotu zamówienia.
Wszelkie odwołania do znaków towarowych, patentów, pochodzenia lub konkretnych modeli urządzeń mają charakter informacyjny i nie mają na celu celem ograniczenia konkurencji.
Zamawiający dopuszcza oferty równoważne, które spełniają powyższe wymagania i zapewniają osiągnięcie tych samych celów funkcjonalnych i jakościowych.”

Otrzymuje następujące brzmienie:

„Zakres zamówienia obejmuje:
1. Implementację ogólnokrajowej sieci SD-WAN – Wdrożenie rozległej sieci SD-WAN, która obejmie wszystkie jednostki Państwowej Straży Pożarnej (PSP) w kraju. Sieć ta zapewni niezawodne, bezpieczne i wydajne połączenia sieciowe pomiędzy jednostkami PSP na różnych szczeblach organizacyjnych, od centralnych, pośrednich, aż po końcowe węzły komunikacyjne.
2. Dostarczenie sprzętu i oprogramowania – Zakres dostawy obejmuje zapewnienie odpowiedniego sprzętu i oprogramowania dla wszystkich szczebli organizacyjnych PSP, w tym:
o Komenda Główna PSP,
o Komendy Wojewódzkie PSP,
o Komendy Powiatowe i Miejskie PSP oraz Jednostki Ratowniczo-Gaśnicze (JRG) i ich posterunki.
Sprzęt i oprogramowanie muszą spełniać wymagania funkcjonalne, wydajnościowe oraz bezpieczeństwa przewidziane w specyfikacji technicznej zamówienia.
3. Integracja z istniejącą infrastrukturą IT PSP – Projekt zakłada pełną integrację nowych rozwiązań z istniejącą infrastrukturą teleinformatyczną Państwowej

Straży Pożarnej, co obejmuje synchronizację z obecnymi systemami, aplikacjami oraz mechanizmami zarządzania i bezpieczeństwa. Wymagana jest kompatybilność z aktualnie funkcjonującymi rozwiązaniami IT w PSP.
4. Wsparcie techniczne i serwis – Wykonawca zobowiązany jest do zapewnienia kompleksowego wsparcia technicznego oraz serwisu przez cały okres obowiązywania umowy.
Obejmuje to naprawy, konserwację oraz aktualizacje oprogramowania i sprzętu, aby zagwarantować ciągłość i stabilność działania wdrożonego systemu.
Dostarczone urządzenia muszą być w pełni kompatybilne z istniejącą infrastrukturą Zamawiającego, w szczególności z systemami zarządzania oraz politykami bezpieczeństwa i routingu. Wymagana jest pełna zgodność z urządzeniami i oprogramowaniem Zamawiającego w następujących obszarach:
1. Kompatybilność sprzętowa:
o Urządzenia muszą być zgodne na poziomie fizycznym, co obejmuje zgodność złącza, interfejsów oraz protokołów komunikacyjnych, tak aby integracja z istniejącą infrastrukturą była płynna i nie wymagała dodatkowych modyfikacji.
2. Kompatybilność programowa:
o Urządzenia muszą współpracować z systemami operacyjnymi, oprogramowaniem zarządzającym oraz istniejącymi politykami bezpieczeństwa. Implementacja dostarczonych urządzeń nie może wymagać modyfikacji obecnych konfiguracji i polityk.
3. Kompatybilność operacyjna:
o Wymagana jest możliwość implementacji polityk bezpieczeństwa i routingu na dostarczonych urządzeniach bez konieczności modyfikacji ich oprogramowania lub konfiguracji sprzętowej. Polityki te muszą być przenoszone w sposób bezproblemowy, zapewniając pełną zgodność z istniejącymi systemami.
W przypadku dostarczenia rozwiązań innych niż te, które obecnie funkcjonują u Zamawiającego, Wykonawca zobowiązany jest na własny koszt dostarczyć, skonfigurować i wdrożyć równoważne rozwiązanie, oparte na urządzeniach pracujących w konfiguracji wysokiej dostępności (HA) w trybach Active/Standby i Active/Active. Dodatkowo rozwiązanie musi być wyposażone w system centralnego zarządzania i monitorowania NG Firewall."

6. Wymagania równoważne dla rozwiązania innego niż funkcjonujące u Zamawiającego:
W pkt. „Rozwiązanie równoważne musi spełniać następujące warunki:" OPZ dodaje się opis parametrów równoważności, które muszą spełniać urządzenia oferowane jako równoważne w następującym brzmieniu:
„Rozwiązanie równoważne musi spełniać następujące warunki:
• Licencje i oprogramowanie: Wymagana jest dostawa odpowiedniej liczby licencji oraz oprogramowania, które umożliwią pełne przeniesienie i implementację

wszystkich polityk oraz konfiguracji, z zachowaniem pełnej funkcjonalności i bezpieczeństwa.
• Serwis i wsparcie techniczne: Wykonawca musi zapewnić serwis gwarancyjny oraz pełne wsparcie techniczne do dnia 7 grudnia 2028 roku. Wsparcie musi być świadczone w trybie 24/7/365, z czasem reakcji na zgłoszenie wynoszącym maksymalnie 2 godziny, a czasem usunięcia awarii wynoszącym maksymalnie 6 godzin od zgłoszenia.
• Szkolenia certyfikacyjne: Wymagane są certyfikowane szkolenia dla personelu Zamawiającego w zakresie obsługi i zarządzania dostarczonym rozwiązaniem, co umożliwi samodzielne utrzymanie systemu przez zespół IT Zamawiającego.
Aktualnie funkcjonujące rozwiązania Zamawiającego obejmują:
• Klaster firewalli nowej generacji: Dwa urządzenia Palo Alto PA-1420, wyposażone w pakiet subskrypcji Core Security, obejmujący zaawansowane zapobieganie zagrożeniom, filtrowanie adresów URL, zabezpieczenia Wildfire, zabezpieczenia DNS oraz SD-WAN (PANPA-1420-BND-CORESEC-5YR) – subskrypcje te obowiązują do dnia 7 grudnia 2028 roku.
• Wsparcie premium: Wsparcie techniczne na najwyższym poziomie (PAN-SVC-BKLN-1420-5YR) dla dwóch urządzeń Palo Alto PA-1420, obejmujące pełną ochronę do 7 grudnia 2028 roku.
• Centralne zarządzanie Panorama: Oprogramowanie Panorama do zarządzania do 100 urządzeń (PAN-PRA-100), które posiada wsparcie techniczne do dnia 7 grudnia 2028 roku.
• Licencje na wirtualne systemy: Licencje na 10 wirtualnych systemów dla 2 urządzeń Palo Alto PA-1420.
• Subskrypcje GlobalProtect: Obejmujące funkcję HIP dla 2000 urządzeń końcowych w konfiguracji HA na 2 urządzenia Palo Alto PA-1420, obowiązujące do dnia 7 grudnia 2028 roku.
Dostarczone urządzenia oraz rozwiązania muszą nie tylko spełniać wskazane wymagania, ale także gwarantować pełną funkcjonalność, zgodność i bezpieczeństwo, co jest kluczowe dla operacyjnej ciągłości i bezpieczeństwa sieci Państwowej Straży Pożarnej.

Warunki równoważności dla urządzeń klasy NGFW (Next-Generation Firewall) posiadanych przez Zamawiającego.
Wszelkie urządzenia uznawane za równoważne muszą spełniać minimalne parametry techniczne określone w niniejszym OPZ, w tym pracować w trybach HA, zapewniać wydajność na poziomie wymaganym przez Zamawiającego oraz być kompatybilne z infrastrukturą istniejącą u Zamawiającego. Rozwiązanie równoważne musi spełniać następujące wymagania minimalne:
Zamawiający dopuszcza urządzenia o równoważnej funkcjonalności, które są specjalizowanymi urządzeniami sieciowymi (tzw. appliance) o możliwościach pracy

w trybach Active/Standby oraz Active/Active, działając jako pojedyncze urządzenie lub para w klastrze wysokiej dostępności (HA) , jako 1 komplet – 2 sztuki pracujące w klastrze w trybie „HA”.
1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
2. Całość sprzętu i oprogramowania musi być dostarczona i zapewniać wsparcie serwisowe przez jednego i tego samego producenta.
3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
a. routera (tzn. w warstwie 3 modelu ISO OSI),
b. mostu (tzn. w warstwie 2 modelu ISO OSI),
c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary) 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.
4. Urządzenia muszą 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.
5. Urządzenia muszą być wyposażone w minimum 2 zasilacze AC 230V pracujące redundantnie.
6. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia tzw. “hot-plug”.
7. Urządzenia firewall muszą 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 realizowana 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.
8. Urządzenia 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.
9. Urządzenia firewall muszą wspierać protokół LACP.
10. Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
11. Urządzenia firewall muszą 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.
12. Polityka zabezpieczeń firewall musi uwzględniać
a. adresy IP źródłowe i docelowe,
b. protokoły i usługi sieciowe,
c. aplikacje,
d. kategorie URL,
e. użytkowników aplikacji i grupy,
f. reakcje zabezpieczeń,
g. logowanie zdarzeń (początek i koniec sesji)
h. strefa wejściowa i wyjściowa
13. Urządzenia firewall muszą 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 3300 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz z aplikacjami przemysłowymi (tzw. ICS/OT) np. DNP3, Modbus.
Urządzenia muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).
14. Urządzenia firewall muszą 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.
15. Urządzenia firewall muszą 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.
16. Urządzenia firewall muszą 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.
17. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
18. Urządzenia firewall muszą 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.

19. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie min. z systemami:
a. Microsoft Active Directory,
b. Microsoft Exchange
c. Terminal Services
d. Syslog
e. Cisco ISE
20. Polityka kontroli dostępu (urządzeń 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.
21. Urządzenia firewall muszą 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.
22. Urządzenia firewall muszą 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.
23. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników.
Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
b. API
24. Urządzenia firewall muszą 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.
25. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.
26. Urządzenia firewall muszą 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.
27. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
28. 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.
29. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF.
30. Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
31. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.
32. Urządzenia firewall muszą 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.
33. 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.
34. 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).
35. 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.
36. 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.

37. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.
38. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.
39. Urządzenia firewall muszą 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).
40. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
41. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
42. Urządzenia firewall muszą zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.
43. Urządzenia firewall muszą obsługiwać funkcję DNS proxy.
44. Urządzenia firewall muszą 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.
45. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
46. Urządzenia firewall dla zdalnego dostępu VPN muszą być wyposażone i umożliwiać następujące funkcjonalności:
a. Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN)
b. Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS i Google Android.
c. Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 10 UWP; iOS 10-17; Google Android 6-14; Linux CentOS, RHEL, Ubuntu;
d. Sprawdzanie informacji o systemie operacyjnym, aktualizacji poprawek OS, aktualizacji oprogramowania antywirusowego itp. (dla systemów PC z Windows).
e. Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów PC z Windows.
f. Możliwość pomijania tunelu zdalnego dostępu VPN dla specyficznych aplikacji, domeny DNS, aplikacji video. Dla podłączających się stacji/laptopów Windows i MacOS.

g. 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.
47. Dostarczane razem z urządzeniami subskrypcje, licencje, gwarancje muszą funkcjonować min. do dnia 7 grudnia 2028 roku.
48. 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.
49. Razem z urządzeniami muszą zostać dostarczone następujące typy i ilości modułów połączeniowych. Ilość dla zestawu 2 urządzeń głównych:
a. Do HA: 4 szt. SFP+ 10GE wariant SR
b. Do LAN: 4 szt. SFP+ 10GE wariant SR
50. Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania, Urządzenie musi być wyposażone w minimum:
a. minimum 4 porty Ethernet RJ45 wspierających 100Mbps/1GE;
b. minimum 4 porty Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps;
c. 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;
d. minimum 2 portów Ethernet SFP (akceptujących moduły 1GE SFP)
e. minimum 8 portów Ethernet SFP+ (akceptujących moduły 10GE SFP+ oraz 1GE SFP)
f. 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.
51. Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 200 GB na potrzeby systemu operacyjnego i logów.
52. 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.
53. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
a. Minimum 9 Gbps dla rozpoznawania i kontroli aplikacji,
b. Minimum 5 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antyspyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia,
c. Minimum 6.5 Gbps wydajności IPSec VPN,
d. Minimum 130 000 nowych sesji na sekundę,
e. Minimum 1.3M równoległych sesji,
f. Minimum 1500 tuneli klienckich VPN,

g. Minimum 2500 sąsiedztw IKE (IPSec).

54. Musi posiadać i obsługiwać bez dodatkowych licencji, 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.

55. Musi umożliwiać zdefiniowanie nie mniej niż 1500 reguł polityk bezpieczeństwa oraz min. 3000 reguł NAT.

56. 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.

57. Urządzenie musi być przeznaczone do montażu w szafie Rack 19”.

58. 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.

59. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.

60. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.

61. 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.

62. 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.

63. Urządzenie musi posiadać funkcję filtrowania URL.

64. Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.

65. 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.

66. Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen.
67. Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania kategorii URL.
68. 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.
69. Administrator musi mieć możliwość konfiguracji jakiego rodzaju typy plików z listy wspieranych przez funkcję Sandbox zostaną wysłane do skanowania przez „Sandbox".
70. 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 infrastrukturze Zamawiającego.
71. 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.
72. Urządzenie musi zapewniać ochronę DNS, co najmniej w zakresie:
a. wykrywanie domen dynamicznych Dynamic DNS;
b. wykrywanie zapytań do domen złośliwych;
c. wykrywanie domen generowanych przez algorytmy DGA;
d. wykrywanie tunelowania złośliwej komunikacji w protokole DNS;
e. wykrywanie DNS Exfiltration or DNS Inflitration;
73. Wraz z urządzeniami Firewall konieczne jest dostarczenie centralnego systemu zarządzania tego samego producenta co wyżej opisane urządzenia firewall.
74. Zamawiający dopuszcza budowę systemu w oparciu o kilka komponentów zarządzania oferowanych przez producenta firewalli i systemu zarządzania pod warunkiem, iż będą one pochodziły od jednego producenta i będą przez niego w całości serwisowane. Zamawiający wymaga, aby wymagania dotyczące liczby zarządzanych firewalli, pojemności przestrzeni dyskowej oraz możliwości rozbudowy były spełnione przez każdy z komponentów tworzących system zarządzania. Należy dostarczyć platformy VM (tzw. VM Appliance).

75. System zarządzania, logowania i raportowania musi zostać dostarczony w postaci urządzenia dedykowanego VM – tzw. Virtual Appliance. (zgodność z Hyper-V i Vmware, instalacja w środowisku wirtualizacji Zamawiającego).
76. System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne:
a. obsługa nie mniej niż 20 klastrów firewalli, z możliwością rozbudowy w przyszłości do 100.
b. obsługa przestrzeni dyskowej minimum 20TB.
77. System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z urządzeń firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach, połączeniach vpn itp.
78. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
79. System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym co najmniej:
a. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych,
b. tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego,
c. zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości email do wybranych osób,
d. tworzenie raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down”.
80. System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami w tym co najmniej:
a. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu,
i. lokalnych (dla wybranych firewalli),
ii. globalnych (dla grup firewalli),
b. umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów).
81. Pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń:
a. umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium,
b. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych.

82. System zarządzania, logowania i raportowania musi udostępniać centralne narzędzia inwentaryzacji i audytu oraz możliwość zarządzania konfiguracjami, w tym co najmniej:
a. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu,
b. umożliwiać tworzenie kopii zapasowych zarządzanych firewalli,
c. umożliwiać dystrybucję i zdalną instalację aktualizacji sygnatur,
d. umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia przed jej zatwierdzeniem,
e. pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli,
f. umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak, aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone,
g. informować o zmianach konfiguracji systemu.
83. System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń.
84. W ramach Zamówienia, Wykonawca przeprowadzi pełną konfigurację i integrację elementów systemu z infrastrukturą Zamawiającego w konfiguracji uzgodnionej z Zamawiającym na etapie wdrożenia. Prace będą obejmowały swoim zakresem, fizyczną instalację urządzeń i oprogramowania będących przedmiotem postępowania (w miejscach wskazanych przez Zamawiającego), integrację z istniejącym systemem teleinformatycznym, konfigurację całego systemu zgodnie z wytycznymi Zamawiającego, konfiguracje dla integracji
z środowiskami: infrastruktury sieciowej, wirtualizacji, systemowej oraz przeszkolenie wyznaczonych pracowników Zamawiającego w zakresie użytkowania i administrowania wdrożonego rozwiązania.
85. Zamawiający wymaga przeszkolenia 4 osób (Administratorów). Czas szkolenia min. 40 godzin szkoleniowych.
86. Zakres szkolenia musi obejmować praktyczne warsztaty w przygotowanym środowisku szkoleniowym.
87. Szkolenie musi być potwierdzone certyfikatem producenta dostarczonego sprzętu (szkolenie certyfikowane).
88. Ostateczne ustalenia z Zamawiającym dotyczące realizacji całego projektu zostaną opisane przez Wykonawcę w dokumencie projektowym, który będzie zawierał szczegóły konfiguracyjne. Dokument zostanie następnie uzgodniony z Zamawiającym.
89. Ponadto Wykonawca będzie świadczył wsparcie merytoryczne do dnia 7 grudnia 2028 roku w zakresie zmian konfiguracji, aktualizacji i rozwiązywania bieżących problemów i awarii.

Zamówienie obejmuje dostawę urządzeń infrastruktury sieci SD-WAN zgodnie z poniższą specyfikacją. W przypadku wskazania znaków towarowych, patentów lub pochodzenia, Zamawiający dopuszcza składanie ofert równoważnych, pod warunkiem że oferowane urządzenia spełniają minimalne wymagania określone w opisie przedmiotu zamówienia.
Wszelkie odwołania do znaków towarowych, patentów, pochodzenia lub konkretnych modeli urządzeń mają charakter informacyjny i nie mają na celu celem ograniczenia konkurencji.
Zamawiający dopuszcza oferty równoważne, które spełniają powyższe wymagania i zapewniają osiągnięcie tych samych celów funkcjonalnych i jakościowych."

7. Dotychczasowy zapis OPZ:

Opis Techniczny:
„Pkt 1. Ogólne wymagania na sprzęt i oprogramowanie urządzeń brzegowych typu NG
Firewall.
30. Urządzenia firewall muszą 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." oraz
„46. Urządzenia firewall muszą 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 wspieraną ilość dla oferowanego modelu urządzeń." oraz
„48. Urządzenia firewall dla zdalnego dostępu VPN muszą umożliwiać następujące funkcjonalności:
a. Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 7/8.1/10/11; MacOS od 10.11 do 14.
b. Jeżeli rozwiązanie danego producenta przewiduje oddzielne wsparcie serwisowe na klienta VPN, należy takie wsparcie przewidzieć na taki sam okres jak wsparcie dla urządzeń dla maksymalnej ilości wspieranych połączeń klienckich VPN dla każdego z urządzeń."

Otrzymuje następujące brzmienie:
„„Pkt 1. Ogólne wymagania na sprzęt i oprogramowanie urządzeń brzegowych typu NG Firewall (Next-Generation Firewall).
30. Urządzenia firewall muszą 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

„46. Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN) dla minimalnej liczby 13 000 użytkowników. 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 minimalną ilość 13 000 połączeń VPN dla oferowanego modelu urządzeń Typ nr 3.” oraz
„48. Urządzenia firewall dla zdalnego dostępu VPN muszą umożliwiać następujące funkcjonalności:
a. Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 7/8.1/10/11; MacOS od 10.11 do 14.
b. Jeżeli rozwiązanie danego producenta przewiduje oddzielne wsparcie serwisowe na klienta VPN, należy takie wsparcie przewidzieć na taki sam okres jak wsparcie dla urządzeń oraz dla minimalnej liczby 13 000 połączeń klienckich VPN dla każdego urządzenia.”

8. Dotychczasowy zapis OPZ:

Pkt 2. Wymagania precyzujące sprzęt i oprogramowanie ze względu na wydajność, rodzaj i ilość portów wej./wyj.:
Pkt 2.1. Wymagania dodatkowe dla urządzeń Typ nr 1 – 4 sztuki (2 pary HA)
„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.”

Otrzymuje następujące brzmienie:
„5. Musi posiadać i obsługiwać bez dodatkowych licencji, nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.”

9. Dotychczasowy zapis OPZ:

Pkt 2. Wymagania precyzujące sprzęt i oprogramowanie ze względu na wydajność, rodzaj i ilość portów wej./wyj.:
Pkt 2.1. Wymagania dodatkowe dla urządzeń Typ nr 1 – 4 sztuki (2 pary HA)
„25. Zewnętrzny sandbox producenta musi być zlokalizowany w Polsce. W przypadku braku dostępności polskiej lokalizacji takiego systemu należy dostarczyć lokalne urządzenia typu sandbox do zainstalowania w sieci Zamawiającego w ilości odpowiadającej ilości urządzeń NG Firewall zawartych w ofercie.”

Otrzymuje następujące brzmienie:
„25. Zewnętrzny sandbox producenta musi być zlokalizowany w Polsce. W przypadku braku dostępności polskiej lokalizacji takiego systemu należy dostarczyć lokalne urządzenia typu sandbox do zainstalowania w sieci Zamawiającego w ilości odpowiadającej ilości urządzeń NG Firewall zawartych w ofercie. (podstawa prawna - z uwagi na przetwarzanie danych zgodnie z SCCO2)"

10. Dotychczasowy zapis OPZ:

Pkt 2.2. Wymagania dodatkowe dla urządzeń Typ nr 2 – 32 sztuki (16 par HA) (urządzenia obsługujące Pośrednie Węzły Komunikacyjne (PWK)).
„4. 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."

Otrzymuje następujące brzmienie:
„4. Musi posiadać i obsługiwać bez dodatkowych licencji, nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń"

11. Dotychczasowy zapis OPZ:

Pkt 2.3. Wymagania dodatkowe dla urządzeń Typ nr 3 – 3 sztuki. (urządzenia obsługujące Węzły VPN).
„4. Musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń."

Otrzymuje następujące brzmienie:
„4. Musi posiadać i obsługiwać bez dodatkowych licencji, nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń."

12. Dotychczasowy zapis OPZ:

Pkt 2.3. Wymagania dodatkowe dla urządzeń Typ nr 3 – 3 sztuki. (urządzenia obsługujące Węzły VPN).
„10. Urządzenia firewall dla zdalnego dostępu VPN muszą dodatkowo umożliwiać

następujące funkcjonalności:."

Otrzymuje następujące brzmienie:
„10. Urządzenia firewall dla zdalnego dostępu VPN muszą być wyposażone i umożliwiać następujące funkcjonalności:"

13. Dotychczasowy zapis OPZ:
Pkt 2.4. Wymagania dodatkowe dla urządzeń Typ nr 4 – 533 sztuk (urządzenia obsługujące Końcowe Węzły Komunikacyjne (KWK))
„4. Musi obsługiwać nie mniej niż 3 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń."

Otrzymuje następujące brzmienie:
„4. Musi posiadać i obsługiwać bez dodatkowych licencji, nie mniej niż 3 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń."

14. Dotychczasowy zapis OPZ:
Pkt 2.5. Wymagania dodatkowe dla urządzeń Typ nr 5 – 33 sztuki (urządzenia zapasowe dla Końcowe Węzły Komunikacyjne (KWK)).
„4. Musi obsługiwać nie mniej niż 3 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń."

Otrzymuje następujące brzmienie:
„4. Musi posiadać i obsługiwać bez dodatkowych licencji, nie mniej niż 3 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń."

15. Dotychczasowy zapis OPZ:
Pkt 3. System Centralnego Zarządzanie i Monitorowania NG Firewall i SD-WAN.
„2. Należy dostarczyć centralny, zunifikowany system zarządzania, logowania zdarzeń i raportowania pochodzący od tego samego producenta co dostarczone urządzenia NG Firewall." oraz
„4. System ma pełnić rolę systemu logowania dla zarządzanych firewalli i systemu centralnego raportowania. W tym celu moduły odpowiedzialne za zbieranie logów muszą zostać zrealizowane z wykorzystaniem protokół konsensusu posiadającego mocne gwarancje spójności (tzw. consensus protocol). Każdy z węzłów

musi obsługiwać przestrzeń dyskową o pojemności nie mniejszej niż 22 TB oraz minimum 20 000 logów na sekundę."

Otrzymuje następujące brzmienie:
„2. Należy dostarczyć centralny, zunifikowany system zarządzania, logowania zdarzeń i raportowania pochodzący od tego samego producenta co dostarczone urządzenia NG Firewall. System logowania może być zrealizowany jako osobne maszyny wirtualne, które ściśle współpracują ze sobą za pomocą natywnych mechanizmów producenta rozwiązania." oraz
„4. System ma pełnić rolę systemu logowania dla zarządzanych firewalli i systemu centralnego raportowania. W tym celu moduł lub moduły odpowiedzialne za zbieranie logów muszą zostać zrealizowane z wykorzystaniem protokół konsensusu posiadającego mocne gwarancje spójności (tzw. consensus protocol). Każdy z węzłów musi obsługiwać przestrzeń dyskową o pojemności nie mniejszej niż 22 TB oraz minimum 20 000 logów na sekundę.
Zamawiający dopuszcza dobór architektury przez wykonawcę, tak aby zapewniona była odpowiednia pojemność systemu logowania i raportowania dla całego systemu."

16. Dotychczasowy zapis OPZ:
Pkt 3. System Centralnego Zarządzanie i Monitorowania NG Firewall i SD-WAN.
„12. System musi umożliwiać tworzenie dynamicznych raportów w czasie rzeczywistym dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down" (pozyskiwania coraz większej ilości informacji o danym zdarzeniu)."

Otrzymuje następujące brzmienie:
„12. System musi umożliwiać tworzenie raportów dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down" (pozyskiwania coraz większej ilości informacji o danym zdarzeniu)."
Jednocześnie Zamawiający załącza jednolity tekst OPZ po zmianach.

Komendant Główny
Państwowej Straży Pożarnej

z up.

Zastępca Komendanta Głównego

Państwowej Straży Pożarnej
st. bryg. Paweł Frysztak
(podpisano kwalifikowanym podpisem elektronicznym)

Załączniki:
1. Opis przedmiotu zamówienia po modyfikacji.