Warszawa dnia 13.08.2020 r.

Strona WWW

Dotyczy postępowania: COI-ZAK.262.20.2020

WYJAŚNIENIA I ZMIANA SIWZ NR 2

Centralny Ośrodek Informatyki, działając jako Zamawiający, w postępowaniu na **rozbudowę infrastruktury systemów nadzoru i bezpieczeństwa (5 części),** na podstawie art. 38 ust. 2 i 4 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz. U. z 2019 r., poz. 1843 z późn. zm.), przedstawia poniżej treść pytań Wykonawców wraz z udzielonymi odpowiedziami oraz zmianę treści SIWZ:

Dotyczy Część I Dostawa i wdrożenie systemu NGFW

PYTANIE NR 25:

Opis przedmiotu zamówienia, III.1.1 OGÓLNE WYMAGANIA DLA DOSTAWY SYSTEMU NGFW
W punkcie 3.4 – zgodność, Zamawiający w zapisach wspólnych dla NGFW i Konsoli zarządzania wymaga certyfikacji Common Criteria wymaga zgodności z „Protection Profile for Stateful Traffic Filter Firewalls" oraz w punkcie 3.5 „Protection Profile for Network Devices". Mając na uwadze, że Konsola NGFW nie jest urządzeniem przetwarzającym ruch sieciowy i jako taka nie może być poddana certyfikacji „Protection Profile for Stateful Traffic Filter Firewalls" natomiast może być podana certyfikacja w ramach „Protection Profile for Network Devices" – prosimy o zmianę zapisów na poprawne i wymaganie dla Konsoli NGFW tylko „Protection Profile for Network Devices" oraz dla urządzeń NGFW obu - „Protection Profile for Network Devices" oraz „Protection Profile for Stateful Traffic Filter Firewalls".

Odpowiedź:

Zamawiający zmienia zapis w pkt III.1.1, wiersz 3 Jednorodność, Szyfrowanie, Dodatkowe kryteria bezpieczeństwa, ppkt 3.4 Rozdziału II SIWZ – Opis Przedmiotu Zamówienia, nadając mu następującą treść: *Urządzenia NGFW powinny posiadać zgodność z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym*,
oraz zmienia zapis w pkt III.1.1, wiersz 3 Jednorodność, Szyfrowanie, Dodatkowe kryteria bezpieczeństwa, ppkt 3.5 Rozdziału II SIWZ – Opis Przedmiotu Zamówienia, nadając mu następującą treść: *Urządzenia NGFW i Konsola NGFW powinny posiadać zgodność z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym.*

PYTANIE NR 26:

Opis przedmiotu zamówienia, III.1.1 OGÓLNE WYMAGANIA DLA DOSTAWY SYSTEMU NGFW
W punkcie 3.4 – Common Criteria.
Ponieważ proces certyfikacji Common Criteria jest procesem bardzo skomplikowanym i długotrwałym - w roku 2020 większość otwartych procesów certyfikacyjnych została opóźniona ze względu na

sytuację z COVID-19. Wnosimy o zaakceptowanie i uznanie jako urządzeń posiadających już certyfikację Common Criteria urządzeń, które: - zostały już zgłoszone do procesu certyfikacji - do odpowiedniego laboratorium certyfikującego, - zostanie przedstawione odpowiednie oświadczenie laboratorium potwierdzające ten fakt, - informacja o trwającej certyfikacji (kolejce oczekujących) jest opublikowana na portalu organizacji danego kraju - wymienionego na liście stowarzyszenia Common Criteria - CCRA (https://www.commoncriteriaportal.org/ccra/members/) - zostanie przedstawiony adres URL pod którym można ten fakt potwierdzić - zostanie dołączony wydruk z tej że listy.

Odpowiedź:

Zamawiający podtrzymuje postanowienia SIWZ i nie wyraża zgody na proponowaną zmianę. Zamawiający wskazuje, że posiadanie certyfikatu Common Criteria stanowi przedmiot kryterium oceny ofert, a rozpoczęcie procesu certyfikacji nie przesądza o zgodności z produktu z certyfikowaną normą dlatego Zamawiający będzie przyznawał punkty w tym kryterium oceny ofert Wykonawcom, którzy zaoferują produkty o już potwierdzonej zgodności z normami Common Criteria.

PYTANIE NR 27:

Opis przedmiotu zamówienia, III.1.2 SZCZEGÓŁOWE WYMAGANIA DLA DOSTAWY NGFW

W punkcie 6.2 oraz 6.2.1 – Interfejsy, Zamawiający wymaga 8 portów SFP oraz dostarczenia 8 wkładek 1000Base-T i 8 wkładek 1000Base-SX. Czy Zamawiający uzna za spełnienie tego punktu, gdy oferowane urządzenie posiada już wbudowane 4 interfejsy miedziane Base-T obsługujące prędkości 100/1GE/10GE oraz wymagane 8 portów SFP przy dostawie 4 wkładek 1000Base-T oraz 8 wkładek 1000Base-SX? Pytanie ma na celu potwierdzenie czy wbudowane 4 interfejsy miedziane 100/1GE/10GE mogą być zaliczone na poczet 4 wkładek SFP 1000Base-T (miedzianych).

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Rozwiązanie przedstawione przez Wykonawcę nie spełni wymagania SIWZ.

PYTANIE NR 28:

Opis przedmiotu zamówienia, III.1.2 SZCZEGÓŁOWE WYMAGANIA DLA DOSTAWY NGFW

W punkcie 14.4 – Kategoryzacja www, Zamawiający wymaga aktualizacji kategorii i wymienia na liście TOR. W przypadku sieci TOR wykorzystanie technologii kategoryzacji/filtracji WWW/URL nie działa - ze względu na ukrywanie komunikacji TOR w szyfrowanej komunikacji. Prosimy o zmianę wymagania w zakresie pozycji TOR. Czy Zamawiający uzna za spełnienie punktu 14.4 dla TOR, jeżeli dostarczone urządzenie NGFW potrafi rozpoznawać i blokować za pomocą mechanizmów rozpoznawania aplikacji: aplikacji tor oraz aplikacja tor2web oraz blokować węzły TOR za pomocą adresów IP - tzw. TOR Nodes za pomocą mechanizmów wymaganych w punkcie 15.4 (tzn. za pomocą Feed-ów z zewnętrznych serwerów).

Odpowiedź:

Zamawiający wymaga aby listę IP TOR Nodes dostarczał m.in. Producent Systemu NGFW oraz ją aktualizował. Rozwiązanie przedstawione przez Wykonawcę nie spełni wymagania SIWZ.

PYTANIE NR 29:

Opis przedmiotu zamówienia, III.1.2 SZCZEGÓŁOWE WYMAGANIA DLA DOSTAWY NGFW

W punkcie 15.2 – podpunkt 2 „reputacji (IP, domen i URL)", Zamawiający wymaga blokowania ruchu sieciowego za pomocą reputacji dla IP, domen i URL. Blokowanie na podstawie reputacji było stosowane w świecie bezpieczeństwa sieciowego w przeszłości. Obecnie przy powszechnym

stosowaniu Public Cloud i dynamicznej dystrybucji ruch sieciowego zastosowanie reputacji IP nie przynosi oczekiwanego efektu. Wnosimy o usunięcie z punktu 15.2 podpunktu o treści „reputacji (IP, domen i URL)" jako nie mającego istotnego wpływu na bezpieczeństwo a ograniczającego listę producentów.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Powyższe wymaganie wynika z potrzeb Zamawiającego. Wedle wiedzy Zamawiającego jest kilku producentów, którzy spełniają powyższe wymagania.

PYTANIE NR 30:

Opis przedmiotu zamówienia, III.1.2 SZCZEGÓŁOWE WYMAGANIA DLA DOSTAWY NGFW
W punkcie 15.6 – Ochrona przed atakami typu flood, Zamawiający wymienia wymaganie „HTTP flood". Zaproponowany zapis ogranicza ilość producentów sieciowych. Prosimy o usunięcie tego zapisu, dla którego ochrona może być realizowana za pomocą wcześniej wymienionego SYN TCP lub dopuszczenie w niego miejsce ICMPv6 (częściej spotykany zapis u producentów sieciowych).

Odpowiedź:

Zamawiający zmienia zapis w pkt III.1.2, wiersz 15 Ochrona NGFW - funkcjonalność, ppkt 15.6 Rozdziału II SIWZ – Opis Przedmiotu Zamówienia, nadając mu następującą treść:
Ochrona przed atakami typu flood:

- *SYN flood,*
- *UDP flood,*
- *IP flood,*
- *ICMP flood.*

PYTANIE NR 31:

Opis przedmiotu zamówienia, III.1.3. WYMOGI DOTYCZĄCE KONSOLI NGFW
W punkcie 19.2 – Generowanie raportów html, pdf. Zamawiający wymaga raportów w formacie html. Ponieważ format ten jest wykorzystywany przez przeglądarkę internetową i przez nią interpretowany – nie pozwala na osiągnięcie powtarzalności i spójności raportów. Prosimy o zmianę wymagania na format np. CSV, który może być wykorzystywany i importowany przez wiele narzędzi i daje powtarzalne i ustandaryzowane źródło danych.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Wedle wiedzy Zamawiającego jest kilku producentów, którzy spełniają powyższe wymagania.

PYTANIE NR 32:

Opis przedmiotu zamówienia, III.1.3. WYMOGI DOTYCZĄCE KONSOLI NGFW
Punkt 19.5 – sprawdzenie wpływu aktualizacji IPS na chroniony ruch sieciowy. Dużo większe znaczenie w procesie utrzymania systemu ma znaczenie Polityka Bezpieczeństwa i obsługa zezwolonych aplikacji niż sam składnik sygnatur IPS. Zasadnym jest aby administrator systemu miał możliwość opóźnienia uruchomienia nowych sygnatur i aplikacji aby wyeliminować możliwe błędy i pomyłki producenta. Prosimy o zmianę bardzo specyficznego zapisu (niż tylko IPS) na wymaganie które zagwarantuje Zamawiającemu możliwość opóźnienia włączenia pobranych aktualizacji (aplikacje i zagrożenia a nie tylko IPS).

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Wedle wiedzy Zamawiającego jest kilku producentów, którzy spełniają powyższe wymagania.

PYTANIE NR 33:

Opis przedmiotu zamówienia, III.1.3. WYMOGI DOTYCZĄCE KONSOLI NGFW

Punkt 19.5 – sprawdzenie wpływu aktualizacji IPS na chroniony ruch sieciowy. Czy możliwość sprawdzenia wpływu aktualizacji rozpoznawanych przez system NGFW aplikacji (bezpośrednio na urządzeniu NGFW) będzie zaakceptowana jako spełniająca te wymaganie?

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Wedle wiedzy Zamawiającego jest kilku producentów, którzy spełniają powyższe wymagania. Rozwiązanie przedstawione przez Wykonawcę nie spełni wymagania SIWZ.

PYTANIE NR 34:

Opis przedmiotu zamówienia, III.1.3. WYMOGI DOTYCZĄCE KONSOLI NGFW

Punkt 19.5 – sprawdzenie wpływu aktualizacji IPS na chroniony ruch sieciowy. Czy Zamawiający zaakceptuje jako spełnienie tego wymagania funkcję powiadamiania przez producenta o aktualizacjach sygnatur i aplikacji dostępny w GUI systemu jako dziennik aktualizacji (tzw. release notes) w połączeniu z dodatkowym bezpośrednim powiadamianiem za pomocą wiadomości wysyłanych przez producenta rozwiązania?

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Wedle wiedzy Zamawiającego jest kilku producentów, którzy spełniają powyższe wymagania. Rozwiązanie przedstawione przez Wykonawcę nie spełni wymagania SIWZ.

PYTANIE NR 35:

Opis przedmiotu zamówienia, III.1.3. WYMOGI DOTYCZĄCE KONSOLI NGFW

W Punkt 19.5 – sprawdzenie wpływu aktualizacji IPS na chroniony ruch sieciowy. Różni producenci w różny sposób realizują proces aktualizacji sygnatur i innych składników bezpieczeństwa systemów NGFW. Z tego względu prosimy o usunięcie punktu 19.5 jako zapisu ograniczającego do producentów którzy dokonują aktualizacji sygnatur IPS jako oddzielnego procesu aktualizacji systemu.

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ. Wedle wiedzy Zamawiającego jest kilku producentów, którzy spełniają powyższe wymagania. Rozwiązanie przedstawione przez Wykonawcę nie spełni wymagania SIWZ.

Dotyczy Rozdziału I SIWZ

PYTANIE NR 36:

Dotyczy SIWZ (Rozdział I_SIWZ_COI.ZAK.262.20.2020)W kryteriach oceny ofert w punktach 23.6 i 23.9 Zamawiający wskazuje strony w języku angielskim. Czy Zamawiający dopuści składanie dokumentów wskazanych w punkcie 23.6 i punkcie 23.9 w języku angielskim bez konieczności przedstawienia tłumaczenia na język polski?

Odpowiedź:

Zamawiający wyraża zgodę. Wykonawca nie musi przedkładać tłumaczenia z języka angielskiego na język polski dokumentów wymienionych w pkt 23.6 i 23.9 Rozdziału I SIWZ – Instrukcja dla Wykonawców.

Zamawiający informuje, że na podstawie art. 38 ust. 4 ustawy Pzp dokonał zmiany następujących postanowień Rozdziału I SIWZ – Instrukcja dla Wykonawców, nadając im następującą treść:

Punkt 15.2.7 uzyskuje brzmienie: „W przypadku zaoferowania Urządzenia NGFW o funkcjonowaniu zgodnym z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym w części I, Zamawiający wymaga przedłożenia odpowiedniego dokumentu potwierdzającego taką zgodność wraz z ofertą."

Punkt 15.2.8 uzyskuje brzmienie: „W przypadku zaoferowania Urządzenia NGFW i Konsoli NGFW o funkcjonowaniu zgodnym z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym w części I, Zamawiający wymaga przedłożenia odpowiedniego dokumentu potwierdzającego taką zgodność wraz z ofertą."

Punkt 23.3 tabela z punktacją dla części I uzyskuje brzmienie:

Nazwa kryterium – dotyczy **Części I**	Waga
Cena	**60%**
Zgodność Urządzenia NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym	**30%**
Zgodność Urządzenia NGFW i Konsoli NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym	**10%**

Punkt 23.6 uzyskuje brzmienie: „Zasady oceny kryterium **Zgodność Urządzenia NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym (S) w zakresie Części I:**

Zamawiający przyzna punkty w kryterium „Zgodność Urządzenia NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym" Wykonawcy, który zaoferuje Urządzenia NGFW o funkcjonowaniu zgodnym z profilem „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym ustanowionym w ramach porozumienia o wzajemnym respektowaniu rezultatów oceny i certyfikacji bezpiecznych produktów informatycznych - CCRA (ang. Common Criteria Recognition Arrangement), opublikowanym na stronie internetowej https://www.commoncriteriaportal.org/pps/collaborativePP.cfm?cpp=1 oraz potwierdzonym odpowiednim dokumentem wystawionym przez jeden z podmiotów uprawnionych i wskazanych na stronie internetowej

https://www.commoncriteriaportal.org/labs/. Zamawiający przyzna punkty według następujących zasad:

1) Dokument może obejmować zgodność z dowolną opublikowaną wersją profilu „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym,
2) Dokument może obejmować dowolny stopień ewaluacji („PP Compliant", EAL1 lub wyżej),
3) Zamawiający przyzna punkty w tym kryterium oceny ofert, jeżeli oferowane przez Wykonawcę Urządzenia NGFW, wskazane w formularzu ofertowym będą zawarte na liście opublikowanej na stronie internetowej https://www.commoncriteriaportal.org/products/,
4) Zamawiający przyzna punkty niezależnie od posiadania przez oferowane Urządzenia NGFW zgodności z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym, stanowiącym przedmiot odrębnego kryterium oceny ofert."

Punkt 23.7 uzyskuje brzmienie: „Zamawiający wskazuje następujące warunki równoważności dla systemu równoważnego dla Common Criteria:

1) System opracowany na podstawie porozumienia podmiotów prawa publicznego, utworzonych w celu realizowania zadań związanych z informatyzacją, z co najmniej 10 krajów w tym co najmniej 5 Państw Członkowskich Unii Europejskiej lub NATO;
2) System i funkcjonuje co najmniej od 10 lat;
3) System obejmuje powoływanie niezależnych podmiotów certyfikujących, wykonujących oceny zgodnie z metodologią przyjętą w ramach tego systemu;
4) System zawiera metodologię ewaluacji i tworzenia wzorców normatywnych zabezpieczeń sprzętu oraz opracowane wzorce dla sprzętów sieciowych oraz sprzętów typu Firewall;
5) System musi obejmować szczegółowe wymagania co najmniej w następujących obszarach: komunikacja z urządzeniami sieciowymi, aktualizacje, aktywność na potrzeby audytu, wymiana danych uwierzytelniających, błędy urządzeń, ochrona fizyczna, polityka bezpieczeństwa, zarządzanie kluczami kryptograficznymi, operacje kryptograficzne, generator liczb losowych, ochrona informacji, identyfikacja i autoryzacja, zarządzanie hasłami, identyfikacja użytkownika, zarządzanie bezpieczeństwem, ochrona kluczowych danych, monitorowanie dostępu;
6) System powinien być ogólnie dostępny, możliwy do zweryfikowania przez Zamawiającego;
7) System został wskazany w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa;
8) Zamawiający uzna jako równoważny system obejmujący zgodność z innym profilem ustanowionym w ramach porozumienia o wzajemnym respektowaniu rezultatów oceny i certyfikacji bezpiecznych produktów informatycznych - CCRA, pod warunkiem, że wykonawca w załączonym dokumencie wykaże brak sprzeczności pomiędzy tym profilem oraz profilem „collaborative Protection Profile for Stateful Traffic Filter Firewalls", a także przedmiotowo istotne różnice pomiędzy profilami, uzasadniające twierdzenie, że profile te nie są sprzeczne, w kontekście wszystkich funkcjonalności oferowanego urządzenia."

Punkt 23.8 uzyskuje brzmienie: „Na potwierdzenie kryterium Zgodność Urządzenia NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls"

lub równoważnym (S) Zamawiający wymaga przedłożenia odpowiedniego dokumentu, o którym mowa w pkt 23.6 powyżej wraz z ofertą.

23.8.1 Punkty zostaną przyznane zgodnie z poniższą tabelą:

Zgodność Urządzenia NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym	**Liczba punktów**
Urządzenia NGFW o nie potwierdzonym funkcjonowaniu zgodnym z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym	0 pkt.
Urządzenia NGFW o funkcjonowaniu zgodnym z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym	30 pkt.

23.8.2 W przypadku nie wskazania przez Wykonawcę w ofercie w sposób jednoznaczny, że oferowane Urządzenia NGFW są zgodne z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym Zamawiający przyjmie, iż Wykonawca nie oferuje Urządzenia NGFW zgodnego z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym.

23.8.3 Maksymalna liczba punktów jakie może uzyskać Wykonawca w tym kryterium to 30 pkt."

Punkt 23.9 uzyskuje brzmienie: „Zasady oceny kryterium **Zgodność Urządzenia NGFW i Konsoli NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym (N) w zakresie Części I:**

Zamawiający przyzna punkty w kryterium „Zgodność Urządzenia NGFW i Konsoli NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym Wykonawcy, który zaoferuje Urządzenia NGFW i Konsolę NGFW o funkcjonowaniu zgodnym z profilem „collaborative Protection Profile for Network Devices" lub równoważnym ustanowionym w ramach porozumienia o wzajemnym respektowaniu rezultatów oceny i certyfikacji bezpiecznych produktów informatycznych - CCRA (ang. Common Criteria Recognition Arrangement), opublikowanym na stronie internetowej https://www.commoncriteriaportal.org/pps/collaborativePP.cfm?cpp=1 oraz potwierdzonym odpowiednim dokumentem wystawionym przez jeden z podmiotów uprawnionych i wskazanych na stronie internetowej https://www.commoncriteriaportal.org/labs/. Zamawiający przyzna punkty według następujących zasad:

1) Dokument może obejmować zgodność z dowolną opublikowaną wersją profilu „collaborative Protection Profile for Network Devices" lub równoważnym,
2) Dokument może obejmować dowolny stopień ewaluacji („PP Compliant", EAL1 lub wyżej),
3) Zamawiający przyzna punkty w tym kryterium oceny ofert, jeżeli oferowane przez Wykonawcę Urządzenia NGFW i Konsola NGFW, wskazane w formularzu ofertowym będą zawarte na liście opublikowanej na stronie internetowej https://www.commoncriteriaportal.org/products/,
4) Zamawiający przyzna punkty niezależnie od posiadania przez oferowane Urządzenia NGFW i Konsolę NGFW zgodności z profilem zabezpieczeń Common Criteria –

„collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym, stanowiącym przedmiot odrębnego kryterium oceny ofert."

Punkt 23.10 uzyskuje brzmienie: „Zamawiający wskazuje następujące warunki równoważności dla systemu równoważnego dla Common Criteria:

1) System opracowany na podstawie porozumienia podmiotów prawa publicznego, utworzonych w celu realizowania zadań związanych z informatyzacją, z co najmniej 10 krajów w tym co najmniej 5 Państw Członkowskich Unii Europejskiej lub NATO;
2) System funkcjonuje co najmniej od 10 lat;
3) System obejmuje powoływanie niezależnych podmiotów certyfikujących, wykonujących oceny zgodnie z metodologią przyjętą w ramach tego systemu,
4) System zawiera metodologię ewaluacji i tworzenia wzorców normatywnych zabezpieczeń sprzętu oraz opracowane wzorce dla sprzętów sieciowych oraz sprzętów typu Firewall;
5) System musi obejmować szczegółowe wymagania co najmniej w następujących obszarach: komunikacja z urządzeniami sieciowymi, aktualizacje, aktywność na potrzeby audytu, wymiana danych uwierzytelniających, błędy urządzeń, ochrona fizyczna, polityka bezpieczeństwa, zarządzanie kluczami kryptograficznymi, operacje kryptograficzne, generator liczb losowych, ochrona informacji, identyfikacja i autoryzacja, zarządzanie hasłami, identyfikacja użytkownika, zarządzanie bezpieczeństwem, ochrona kluczowych danych, monitorowanie dostępu;
6) System powinien być ogólnie dostępny, możliwy do zweryfikowania przez Zamawiającego;
7) System został wskazany w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa;
8) Zamawiający uzna jako równoważny system obejmujący zgodność z innym profilem ustanowionym w ramach porozumienia o wzajemnym respektowaniu rezultatów oceny i certyfikacji bezpiecznych produktów informatycznych - CCRA, pod warunkiem, że wykonawca w załączonym dokumencie wykaże brak sprzeczności pomiędzy tym profilem oraz profilem „collaborative Protection Profile for Stateful Traffic Filter Firewalls", a także przedmiotowo istotne różnice pomiędzy profilami, uzasadniające twierdzenie, że profile te nie są sprzeczne, w kontekście wszystkich funkcjonalności oferowanego urządzenia."

Punkt 23.11. uzyskuje brzmienie: „Na potwierdzenie kryterium Zgodność Urządzenia NGFW i Konsoli NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym (N) Zamawiający wymaga przedłożenia odpowiedniego dokumentu, o którym mowa w pkt 23.9 wraz z ofertą.

23.11.1 Punkty zostaną przyznane zgodnie z poniższą tabelą:

Zgodność Urządzenia NGFW i Konsoli NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym	**Liczba punktów**
Urządzenia NGFW i Konsola NGFW o nie potwierdzonym funkcjonowaniu zgodnym z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym	0 pkt.

Urządzenia NGFW i Konsolę NGFW o funkcjonowaniu zgodnym z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym	10 pkt.

23.11.2 W przypadku nie wskazania przez Wykonawcę w ofercie w sposób jednoznaczny, że oferowane Urządzenia NGFW i Konsola NGFW są zgodne z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym Zamawiający przyjmie, iż Wykonawca nie oferuje Urządzenia NGFW i Konsoli NGFW zgodnego z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym.

23.11.3 Maksymalna liczba punktów jakie może uzyskać Wykonawca w tym kryterium to 10 pkt."

Punkt 23.17 uzyskuje brzmienie: „Obliczenie łącznej liczby punktów uzyskanych przez Wykonawcę **w zakresie części I** (spośród ofert podlegających ocenie) zostanie dokonane na podstawie sumy uzyskanych punktów w kryterium **„Cena"**, **„Zgodność Urządzenia NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym** i **„Zgodność Urządzenia NGFW i Konsoli NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym** zgodnie ze wzorem:

R = C + S + N

gdzie:

C - liczba punktów przyznanych Wykonawcy w kryterium „Cena",

S - liczba punktów przyznanych Wykonawcy w kryterium „Zgodność Urządzenia NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls" lub równoważnym,

N - liczba punktów przyznanych Wykonawcy w kryterium „Zgodność Urządzenia NGFW i Konsoli NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices" lub równoważnym,"

Zamawiający informuje, że na podstawie art. 38 ust. 4 ustawy Pzp dokonał zmiany Rozdziału IV - Formularz ofertowy wraz z załącznikami dla Część I: dostawa i wdrożenie systemu NGFW w formularzu ofertowym w pkt 4.8 oraz 4.9. W załączeniu skorygowany Rozdział IV - Formularz ofertowy wraz z załącznikami.

Ponadto Zamawiający informuje, że na podstawie art. 38 ust. 4 ustawy Pzp przedłuża termin składania ofert do dnia 31/08/2020 r. do godz. 11:00.

Odpowiednio zmianie ulegają zapisy w rozdziale I SIWZ:

18. Miejsce oraz termin składania i otwarcia ofert

18.1 Ofertę należy złożyć za pośrednictwem formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionego również na miniPortalu w nieprzekraczalnym terminie:

do dnia	**31/08/2020 r.**	do godz.	**11:00**

18.3 Otwarcie ofert nastąpi poprzez transmisję online na kanale prowadzonym przez Zamawiającego w serwisie YouTube:
https://www.youtube.com/channel/UC_QmMH9HJA6RMc7oYKXVFBg

w dniu	**31/08/2020 r.**	o godz.	**13:00**

Niniejsze wyjaśnienia i zmiany stanowią integralną część SIWZ.

/-/ Stanisław Chajewski
Dyrektor Departamentu Prawnego