Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zakup i wdrożenie urządzenia deszyfrującego ruch sieciowy TLS.

I. Urządzenie deszyfrujące ruch sieciowy TLS– minimalne wymagania

1. Urządzenie wraz z zainstalowanym systemem operacyjnym umożliwi automatyczne rozszywanie ruchu TLS w celu przekazania go w trybie in-line do systemów analizy oraz blokowania szkodliwego oprogramowania a następnie ruch zostanie powrotnie przekazany do tego samego urządzenia rozszywającego, zostanie zaszyfrowany i przekazany do dalszej komunikacji.
   Rozwiązanie musi umożliwiać realizację procesu:

   ruch szyfrowany → deszyfrowanie → urządzenia bezpieczeństwa → ponowne szyfrowanie → dalsza transmisja

   dla obu kierunków transmisji.

   Urządzenie musi umożliwiać definiowanie kolejności oraz liczby systemów bezpieczeństwa znajdujących się w łańcuchu przetwarzania ruchu.

2. Urządzenie musi umożliwiać przekazywanie odszyfrowanego ruchu TLS/SSL w trybie inline do co najmniej trzech kolejnych systemów bezpieczeństwa, z możliwością określenia kolejności ich występowania w łańcuchu przetwarzania.
   Rozwiązanie musi umożliwiać realizację następującego logicznego modelu przepływu:

   deszyfrator TLS → system bezpieczeństwa 1 → system bezpieczeństwa 2 → system bezpieczeństwa 3 → deszyfrator TLS

   oraz analogicznego przepływu dla przeciwnego kierunku transmisji.

   Oferowane urządzenie musi umożliwiać współpracę z istniejącymi systemami bezpieczeństwa Zamawiającego, w szczególności z:
   - IPS Forcepoint,
   - Next Generation Firewall FortiGate,
   - Fidelis Cybersecurity Sensor Direct,

   z wykorzystaniem standardowych interfejsów i mechanizmów transmisji Ethernet.

   Dopuszcza się realizację połączeń pomiędzy urządzeniem deszyfrującym a systemami bezpieczeństwa z wykorzystaniem interfejsów miedzianych lub optycznych, odpowiednio do możliwości oferowanego rozwiązania.
   Obecna infrastruktura Zamawiającego wykorzystuje połączenia 1 Gb/s

realizowane za pomocą interfejsów RJ45. Oferowane rozwiązanie musi umożliwiać wykorzystanie istniejącej infrastruktury oraz zapewniać możliwość jej rozbudowy.

a. Urządzenie musi umożliwiać realizację połączeń za pomocą interfejsów:
   - miedzianych Ethernet,
   - optycznych Ethernet.
b. Oferowane rozwiązanie musi obsługiwać interfejsy o przepustowości co najmniej:
   - 1 Gb/s,
   - 10 Gb/s,
   - 25 Gb/s,

   odpowiednio do zastosowanego typu interfejsu.
c. Urządzenie musi umożliwiać zastosowanie modułów/interfejsów SFP, SFP+ lub SFP28 odpowiednich do wymaganej przepustowości.
   Rozwiązanie musi umożliwiać zastosowanie optyki zgodnej z infrastrukturą Zamawiającego, w szczególności dla transmisji wielomodowej MM w standardzie SR.
d. Dla połączeń optycznych Zamawiający przewiduje wykorzystanie patchcordów zakończonych złączami LC-LC Duplex, odpowiednich do zastosowanego typu włókna i standardu optycznego.
e. Z uwagi na lokalizację urządzeń w jednej szafie teleinformatycznej wymagane jest zapewnienie możliwości wykonania połączeń z wykorzystaniem patchcordów o długości nie większej niż 2 m.
f. Urządzenie musi umożliwiać realizację łańcucha inline składającego się z co najmniej trzech systemów bezpieczeństwa, z możliwością określenia kolejności przepływu ruchu.

3. Oferowane urządzenie musi zapewniać możliwość zwiększenia przepustowości oraz przejścia z interfejsów miedzianych na optyczne bez konieczności zmiany funkcjonalnego modelu realizacji inspekcji inline.
   Rozbudowa musi zachować możliwość:
   - deszyfrowania ruchu TLS/SSL,
   - przekazywania odszyfrowanego ruchu do systemów bezpieczeństwa,
   - odbierania ruchu z systemów bezpieczeństwa,
   - ponownego szyfrowania ruchu,
   - przekazywania ruchu do dalszej komunikacji.

   Dopuszcza się realizację rozbudowy poprzez wymianę lub dodanie interfejsów, modułów, kart lub innych elementów sprzętowych przewidzianych przez producenta dla oferowanej platformy.

4. Wykrywanie oraz deszyfrowanie komunikacji TLS/SSL musi być realizowane przez dedykowane urządzenie sprzętowe lub dedykowany moduł sprzętowy przeznaczony przez producenta do realizacji funkcji inline TLS/SSL decryption.

   Nie dopuszcza się rozwiązania, w którym funkcja deszyfrowania jest realizowana wyłącznie przez oprogramowanie uruchomione na ogólnym serwerze bez dedykowanej funkcji sprzętowej producenta.
5. Urządzenie musi zapewniać następującą minimalną wydajność dla ruchu TLS/SSL w trybie inline:

a. Przepustowość deszyfrowania ruchu TLS/SSL w konfiguracji bez dodatkowych urządzeń bezpieczeństwa w łańcuchu inspekcji: **minimum 4,8 Gbps**,
b. Przepustowość deszyfrowania ruchu TLS/SSL przy zastosowaniu co najmniej jednego zewnętrznego systemu bezpieczeństwa pracującego inline: **minimum 3,5 Gbps**,
c. Przepustowość deszyfrowania ruchu TLS/SSL przy zastosowaniu co najmniej dwóch zewnętrznych systemów bezpieczeństwa pracujących inline: **minimum 2,8 Gbps,**
d. Urządzenie musi umożliwiać utworzenie łańcucha obejmującego co najmniej trzy systemy bezpieczeństwa pracujące inline.
   Oferent musi podać deklarowaną przez producenta przepustowość dla konfiguracji obejmującej trzy systemy bezpieczeństwa pracujące inline.
   Dodanie kolejnych systemów bezpieczeństwa do łańcucha nie może powodować ograniczenia możliwości realizacji funkcji inline TLS/SSL decryption poniżej wartości wymaganej dla danego scenariusza.
e. Urządzenie musi obsługiwać minimum: **6 000 nowych sesji TLS/SSL na sekundę (TPS)** w konfiguracji inline.
f. W przypadku podawania parametrów wydajnościowych przez producenta w odniesieniu do określonej metodologii testowej, oferent zobowiązany jest wskazać:
   - model urządzenia,
   - zastosowaną konfigurację sprzętową,
   - wersję oprogramowania,
   - zastosowaną metodę szyfrowania,
   - sposób pomiaru TPS,
   - warunki testu,
   - czy podana wartość dotyczy ruchu jednokierunkowego czy dwukierunkowego.

   Parametry wydajnościowe muszą dotyczyć oferowanego modelu i oferowanej konfiguracji urządzenia.

6. Urządzenie musi wspierać:
   a. TLS 1.3 oraz TLS 1.2.
   b. Protokoły aplikacyjne HTTP/1.1 oraz HTTP/2.
   c. Rozpoznawanie ruchu TLS/SSL niezależnie od zastosowanego numeru portu TCP.
   d. Rozpoznawanie ruchu aplikacyjnego na podstawie analizy protokołu, a nie wyłącznie na podstawie numeru portu.
   e. Rozpoznawanie ruchu QUIC/HTTP/3 oraz możliwość zastosowania wobec niego skonfigurowanej polityki bezpieczeństwa, w szczególności:
      - przepuszczenia ruchu,
      - zablokowania ruchu,
      - wyłączenia ruchu z procesu deszyfracji,
      - skierowania ruchu do zdefiniowanego procesu dalszego przetwarzania,
      - zgodnie z funkcjonalnościami oferowanego rozwiązania.

      Nie wymaga się deszyfrowania QUIC/HTTP/3, o ile producent nie zapewnia takiej funkcjonalności.
7. Urządzenie musi zapewniać mechanizm zapewniający ciągłość przepływu ruchu w przypadku:

- awarii urządzenia,
- awarii pojedynczego interfejsu,
- utraty zasilania,
- utraty komunikacji z urządzeniem bezpieczeństwa,

poprzez sprzętowy mechanizm bypass, Fail-to-Wire, Fail-to-Network, Fail-to-Appliance lub rozwiązanie funkcjonalnie równoważne.
Mechanizm musi zapewniać automatyczne przekazanie ruchu z pominięciem niedostępnego elementu infrastruktury, zgodnie z konfiguracją urządzenia.

8. Urządzenie musi zapewniać możliwość realizacji wymaganej topologii inline z wykorzystaniem interfejsów miedzianych oraz optycznych.
   Oferowane rozwiązanie musi obsługiwać:
   a. co najmniej 4 interfejsy Ethernet 1 Gb/s umożliwiające realizację połączeń miedzianych RJ45;
   b. co najmniej 4 interfejsy optyczne obsługujące przepustowości 1/10/25 Gb/s, z wykorzystaniem odpowiednich modułów SFP/SFP+/SFP28;
   c. jednoczesną pracę interfejsów miedzianych i optycznych;
   d. standardy optyczne kompatybilne z infrastrukturą Zamawiającego, w szczególności 10/25 Gb/s SR dla światłowodu wielomodowego.

   Dopuszcza się realizację wymaganej liczby interfejsów poprzez zastosowanie modułów, kart lub innych elementów rozszerzających przewidzianych przez producenta dla oferowanego modelu, pod warunkiem zachowania wymaganej funkcjonalności oraz wydajności.

9. Urządzenie musi zapewniać zarządzanie certyfikatami wykorzystywanymi do realizacji funkcji TLS/SSL decryption, w szczególności:
   - automatyczne generowanie certyfikatów self-signed;
   - import certyfikatów oraz kluczy prywatnych;
   - generowanie CSR;
   - możliwość wykorzystania certyfikatów wystawionych przez CA Zamawiającego;
   - możliwość zarządzania certyfikatami wykorzystywanymi do deszyfrowania ruchu TLS/SSL.

10. Urządzenie musi posiadać mechanizm kategoryzacji domen/hostów umożliwiający wykorzystanie kategorii w politykach bezpieczeństwa oraz politykach deszyfracji.
    Mechanizm musi umożliwiać wyłączenie z procesu deszyfracji ruchu kierowanego do określonych kategorii domen, w szczególności kategorii:
    - finansowych,
    - medycznych,
    - religijnych,
    - rządowych,

    lub równoważnych kategorii zdefiniowanych w bazie producenta.
    Baza kategorii musi być aktualizowana przez producenta.
    System musi umożliwiać:
    - tworzenie własnych kategorii,
    - definiowanie własnych list domen,
    - dodawanie wyjątków,

- wykorzystanie kategorii w politykach deszyfracji.

11. Urządzenie musi umożliwiać budowanie polityk dopuszczania, blokowania, pomijania procesu deszyfracji lub kierowania ruchu do określonego łańcucha bezpieczeństwa na podstawie co najmniej:
    a. adresu IP źródłowego i docelowego, w tym podsieci;
    b. nazwy domeny, w tym nazw zawierających wildcard, np.:
        - *.uprp.gov.pl;
    c. kategorii domen/hostów;
    d. identyfikacji aplikacji lub protokołu warstwy aplikacyjnej L7;
    e. numeru portu oraz protokołu transportowego;
    f. kombinacji co najmniej dwóch spośród powyższych kryteriów.
    g. Polityki muszą umożliwiać co najmniej:
        - Allow / White List,
        - Block / Black List,
        - Bypass / wyłączenie z deszyfracji,
        - skierowanie ruchu do określonego łańcucha urządzeń bezpieczeństwa.

II. Wdrożenie urządzenia deszyfrującego ruch sieciowy TLS – minimalne wymagania

1. Wykonawca zobowiązany jest do:
    a) Instalacji i konfiguracji urządzenia w infrastrukturze Zamawiającego w trybie in-line,
    b) Wgrania i skonfigurowania na urządzeniu certyfikatów używanych do publikacji usług Zamawiającego dostępnych z Internetu, w celu umożliwienia deszyfracji ruchu przychodzącego z Internetu do usług Zamawiającego,
    c) Wgrania i skonfigurowania na urządzeniu certyfikatu, który będzie wykorzystywany do deszyfracji ruchu wychodzącego ze stacji roboczych i serwerów Zamawiającego do Internetu. Wykonawca zobowiązany jest zapewnić, aby certyfikat ten był zaufany na wszystkich stacjach roboczych i serwerach (np. poprzez dystrybucję GPO lub inne metody centralnej dystrybucji), tak aby ich ruch mógł być skutecznie deszyfrowany,
    d) Wykonawca zobowiązany jest do wdrożenia urządzenia w sposób zapewniający pełną funkcjonalność automatycznego deszyfrowania ruchu TLS/SSL, jego przekazania w trybie in-line do systemów analizy bezpieczeństwa i blokowania zagrożeń, a następnie ponownego zaszyfrowania ruchu i przekazania go do dalszej komunikacji w sieci Zamawiającego.
    e) Konfiguracji urządzenia zgodnie z wymaganiami funkcjonalnymi i wydajnościowymi,
    f) Konfiguracji list wykluczeń z deszyfrowania ruchu TLS (adresy IP, nazwy domen) na podstawie reguł i list wykluczeń używanych obecnie w funkcjonującym urządzeniu deszyfrującym TLS,
    g) Konfiguracji mechanizmu kategoryzacji domen na urządzeniu, z wykorzystaniem list domyślnych (finansowe, medyczne, religijne,

rządowe) dostarczanych i aktualizowanych przez producenta w celu wykluczenia wskazanych domen z procesu deszyfrowania ruchu TLS zgodnie z wymaganiami Zamawiającego.

2. Wszystkie prace muszą być realizowane przy współudziale pracowników Zamawiającego, bez przerywania ruchu produkcyjnego.
3. Wykonawca przeprowadzi testy poprawności działania mechanizmu deszyfrowania ruchu TLS dla ruchu przychodzącego i wychodzącego. Wykonawca zweryfikuje dostępność usług, poprawne działanie aplikacji i wydajność przepływu ruchu. Wyniki testów muszą być udokumentowane, a ewentualne problemy opisane wraz z podjętymi działaniami korygującymi.
4. Wykonawca zobowiązany jest do skonfigurowania urządzenia w sposób zapewniający monitorowanie wszystkich portów in-line oraz automatyczne utrzymanie przepływu ruchu w przypadku awarii pojedynczego portu lub utraty łączności, np. poprzez sprzętowy bypass lub inne rozwiązanie gwarantujące nieprzerwaną transmisję ruchu. Wykonawca przeprowadzi testy poprawności działania mechanizmu oraz udokumentuje konfigurację i procedury postępowania w sytuacjach awaryjnych.
5. Wykonawca zobowiązany jest do przygotowania dokumentacji powykonawczej, która musi zawierać:
    a) Opis, schemat architektury i przepływów ruchu sieciowego,
    b) Szczegółową konfigurację urządzenia, polityk oraz sposób instalacji i generowania certyfikatów,
    c) Instrukcję administracyjną dotyczącą obsługi i utrzymania rozwiązania,
    d) Procedury awaryjne oraz plan ciągłości działania systemu.
6. Wykonawca zobowiązany jest do przeprowadzenia technicznych warsztatów szkoleniowych dla minimum dwóch administratorów Zamawiającego, obejmujących wdrożone elementy zaimplementowanego systemu bezpieczeństwa. Warsztaty powinny trwać co najmniej dwa dni po min. 8 godzin dziennie i mieć formę praktyczną, umożliwiającą uczestnikom nabycie wiedzy oraz umiejętności niezbędnych do samodzielnej administracji i eksploatacji wdrożonych rozwiązań. Warsztaty muszą być przeprowadzone w formie stacjonarnej na terenie miasta Warszawa. Wykonawca w trakcie trwania warsztatów musi zapewnić uczestnikom napoje oraz co najmniej jeden ciepły posiłek.

III. Zasady wsparcia technicznego i eksploatacyjnego dla urządzenia deszyfrującego ruch sieciowy TLS

1. W ramach przedmiotu zamówienia wymagany jest zakup 12 miesięcznego pakietu wsparcia producenta dla oferowanego urządzenia deszyfrującego ruch sieciowy TLS oraz odpowiednich licencji dla wszystkich dostarczanych komponentów systemu,
2. Urządzenie oraz wszystkie wymagane licencje muszą być objęte minimum 12-miesięcznym serwisem producenta i wykonawcy, obejmującym:
    a) Dostęp do aktualizacji systemu operacyjnego, oprogramowania

urządzenia oraz baz kategorii domen,

b) Wsparcie techniczne świadczone przez producenta lub autoryzowanego przedstawiciela producenta, w celu diagnozy i rozwiązania problemów lub awarii związanych z działaniem urządzenia,
c) Wymianę sprzętu w przypadku awarii w całym okresie wsparcia.

3. Zakres wsparcia świadczonego przez Wykonawcę lub autoryzowanego przedstawiciela producenta:
    a) Wykonawca zapewni bieżącą obsługę administracyjną i techniczną urządzenia, w szczególności:
        - aktualizację certyfikatów używanych do deszyfracji ruchu,
        - diagnozę problemów z deszyfrowaniem i przekazywaniem ruchu do systemów analizy bezpieczeństwa,
        - wsparcie w integracji z innymi elementami infrastruktury bezpieczeństwa,
        - konsultacje i rekomendacje dotyczące optymalizacji wydajności i konfiguracji,
        - podejmowanie działań naprawczych w przypadku wystąpienia awarii lub usterki, w tym diagnozę przyczyny, przywrócenie prawidłowego działania urządzenia oraz weryfikację poprawności funkcjonowania po usunięciu problemu.