**OPIS PRZEDMIOTU ZAMÓWIENIA**

Zamówienie ma na celu dostarczenie urządzenia dla systemu bezpieczeństwa Data Center (centrum przetwarzania danych) budowanego w ramach Systemu Wspomagania Decyzji (SWD) dla Państwowej Straży Pożarnej – DC SWD PSP.

Zamówienie stanowi uzupełnienie pierwotnych założeń realizowanych w 2018 roku w ramach zamówienia „Dostawa urządzeń dla systemu bezpieczeństwa DC SWD PSP”, które ze względu na brak środków nie zostało w pełni zrealizowane.

1. **Ogólny opis przedmiotu zamówienia**
2. Przedmiotem zamówienia jest:
   1. wykonanie dostawy sprzętu, oprogramowania i licencji,
   2. zapewnienie co najmniej 24 miesięcznego okresu gwarancji i serwisu (w tym upgrade oprogramowania urządzeń, sygnatury IPS oraz anty malware),
   3. podłączenie i konfiguracji w klastrze HA do infrastruktury sieciowej Zamawiającego,
3. Zamawiający oczekuje dostawy i wdrożenia przedmiotu umowy w siedzibie Komendy Głównej Państwowej Straży Pożarnej przy ul. Podchorążych 38, w Warszawie (00‑463).
4. Zamawiający posiada obecnie szereg urządzeń Cisco FirePower zarządzanych   
   z poziomu konsoli zarządzającej Cisco FMCv. Celem postępowania jest dostawa urządzenia FPR2130 oraz podłączenie go do infrastruktury DC SWD PSP, a także połączenie go w klaster HA z drugim urządzeniem FPR2130 będącym w posiadaniu Zamawiającego.
5. **Realizacja zamówienia**
   1. Wykonanie dostawy sprzętu, oprogramowania i licencji urządzenia oraz instalacja i konfiguracja, wg poniższej specyfikacji:
      1. Urządzenie sieciowe firewall z licencją URL Filtering, IPS oraz anty-malware, wyposażone w dwa zasilacze (kable zasilające do UPS) – 1 kompl.,

|  |  |
| --- | --- |
| Parametry i wymagania minimalne | Wypełnia Wykonawca podając oferowane rozwiązania (nazwa, model typ, konkretne parametry) lub akceptując parametry poprzez wpisanie TAK |
| Nazwa oferowanego urządzenia |  |
| Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall) |  |
| Urządzenie wyposażone w 12 portów 10/100/1000BaseT Gigabit Ethernet oraz 4 porty 10Gigabit Ethernet SFP+ |  |
| Dodatkowy slot na moduły sieciowe umożliwiający rozbudowę o dodatkowe 8 portów 10Gigabit Ethernet SFP+ |  |
| Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1.000 sieci VLAN |  |
| Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band |  |
| Urządzenie wyposażone w port USB 2.0 |  |
| Zasilacze redundantne umożliwiające zasilanie prądem przemiennym 230V |  |
| Możliwość montażu w szafie rack 19” (dołączone niezbędne elementy montażowe) |  |
| Wysokość urządzenia 1RU |  |
| Wydajność urządzenia dla uruchomionych modułów firewall’a oraz kontroli aplikacji (AVC) – 4.5Gb/s |  |
| Wydajność urządzenia dla uruchomionych modułów kontroli aplikacji (AVC) oraz systemu IPS – 4.5Gb/s |  |
| Maksymalna liczba sesji (z kontrolą aplikacji) na poziomie 2.000.000 z możliwością zestawiania co najmniej 24.000 nowych połączeń na sekundę |  |
| Możliwość pracy jako brama VPN z wydajnością 1.5Gb/s |  |
| Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej |  |
| Możliwość uruchomienia urządzenia w trybie firewall’a L3, jak i w trybie transparentym |  |
| Urządzenie obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP) |  |
| Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory |  |
| Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) |  |
| Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby |  |
| Urządzenie zapewnia funkcjonalność tzw. Firewall’a Next-Generation w zakresie:   * systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control) * systemu IPS * systemu antymalware * systemu filtracji adresów URL |  |
| System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:   * Wiedza o użytkownikach – uwierzytelnienie * Wiedza o urządzeniach – pasywne skanowanie ruchu * Wiedza o urządzeniach mobilnych * Wiedza o aplikacjach wykorzystywanych po stronie klienta * Wiedza o podatnościach * Wiedza o bieżących zagrożeniach * Baza danych URL |  |
| System posiada otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM |  |
| System wykrywania aplikacji AVC zapewniający:   * możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji * możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług * wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji * współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach |  |
| System IPS zapewniający:   * możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system) * możliwość pracy w trybie pasywnym (IDS) |  |
| System IPS zapewniający możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:   * złośliwe oprogramowanie * skanowanie sieci * ataki na usługę VoIP * próby przepełnienia bufora * ataki na aplikacje P2P * zagrożenia dnia zerowego, itp. |  |
| System IPS zapewniający możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna) |  |
| System IPS zapewniający wiele sposobów wykrywania zagrożeń w tym:   * sygnatury ataków opartych na exploitach * reguły oparte na zagrożeniach * mechanizm wykrywania anomalii w protokołach * mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego |  |
| System IPS zapewniający możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu |  |
| System IPS zapewniający mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives) |  |
| System IPS zapewniający możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń |  |
| System IPS zapewniający wiele możliwości reakcji na zdarzenia w tym takie, jak:   * tylko monitorowanie * blokowanie ruchu zawierającego zagrożenia * zastąpienie zawartości pakietów * zapisywanie pakietów |  |
| System IPS zapewniający możliwość detekcji ataków i zagrożeń opartych na protokole IPv6 |  |
| System IPS zapewniający możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:   * systemach operacyjnych * serwisach * otwartych portach, aplikacjach * zagrożeniach |  |
| System IPS zapewniający możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych |  |
| System IPS zapewniający możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp. |  |
| System IPS zapewniający możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji |  |
| System IPS zapewniający możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego |  |
| System IPS zapewniający mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne |  |
| System IPS zapewniający możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie |  |
| System IPS zapewniający obsługę reguł Snort |  |
| System IPS zapewniający możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS |  |
| System IPS zapewniający mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise) |  |
| System IPS zapewniający mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa |  |
| Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:   * pliki systemowe * pliki graficzne * pliki PDF * pliki wykonywalne * pliki multimedialne * pliki pakietu Office * pliki skompresowane |  |
| Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download |  |
| Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez   * sprawdzenie reputacji plików w systemie globalnym * sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze) * statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu |  |
| Urządzenie zapewnia możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:   * pliki wolne od złośliwego kodu * pliki zawierające złośliwy kod * pliki podejrzane * pliki o własnej, zdefiniowanej przez użytkownika kategorii |  |
| Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna) |  |
| Możliwość rozbudowy podsystemu antymalware o agenta instalowanego na stacjach roboczych i serwerach. Konsola zarządzająca posiadająca możliwość wyświetlenia szczegółowej trajektorii transferu danego pliku po monitorowanej sieci oraz korelacji zdarzeń przychodzących z rozwiązania antymalware rezydującego na serwerach i stacjach roboczych |  |
| System filtracji URL zapewniający:   * kategoryzację stron – w co najmniej 70 kategoriach * bazę URL o wielkości nie mniejszej niż 250 mln URL |  |
| Technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania   * Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny * Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego * Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności |  |

1. Zapewnienie minimum 24 miesięcznego okresu gwarancji i serwisu
2. Wykonawca w ramach umowy zapewni co najmniej 24 miesięcy gwarancji na urządzenia. Ww. gwarancja musi być oparta o świadczenia gwarancyjne producenta urządzeń. Gwarancja fabryczna będzie realizowana przez autoryzowany serwis producenta w trybie „naprawa/wymiana urządzenia w następnym dniu roboczym”. Wraz z dostawą należy dołączyć oświadczenie producenta/ów o wykupieniu ww. gwarancji przez Wykonawcę.
3. Gwarancja zaczyna swój bieg od daty podpisania przez Zamawiającego protokołu odbioru przedmiotu zamówienia podpisanego bez zastrzeżeń.
4. **Instalacja**

Zamawiający oczekuje, że w ramach dostawy Wykonawca wykona montaż urządzeń we wskazanej lokalizacji oraz skonfiguruje i uruchomi klaster HA. Należy również dokonać aktualizacji firmaware do najnowszej wersji oraz uruchomić licencje IPS, anty-malware oraz URL filtering. Wykonawca dokona również podłączenia urządzeń do konsoli zarządzającej FMC. Całość tych działań będzie nadzorowana przez BIŁ KG PSP. Termin instalacji i uruchomienia zostanie podany po dostarczeniu urządzeń, w późniejszym czasie.

1. **Opis równoważności sprzętu, oprogramowania i licencji.**

Zamawiający dopuszcza możliwość składania ofert równoważnych w przypadkach, w których Zamawiający wskazuje znaki towarowe, patent lub pochodzenie przedmiotu zamówienia, z zachowaniem przez Wykonawcę zasad i wymogów opisanych wyżej. Wpisanie znaków towarowych jest uzasadnione specyfiką przedmiotu zamówienia i Zamawiający nie może opisać przedmiotu zamówienia za pomocą innych, dostatecznie dokładnych określeń. Użyte w specyfikacji określenia wskazujące znaki towarowe, patent symbol producenta lub pochodzenie przedmiotu zamówienia należy odczytywać z wyrazami „lub równoważne”. Wykonawca oferując przedmiot równoważny do opisanego w specyfikacji jest zobowiązany zachować równoważność w zakresie parametrów użytkowych, funkcjonalnych i jakościowych, które muszą być na poziomie nie niższym, niż parametry wskazane przez Zamawiającego, oraz winien przedstawić dowody potwierdzające równoważność oferowanego przedmiotu zamówienia.

1. **Inne**
2. Dodatkowe wymagania Zamawiającego:
   1. Razem z urządzeniem Wykonawca dostarczy:

- Wkładka 10 GBase-LR SFP - 4 sztuki,

- Wkładka 10 GBase-SR SFP - 6 sztuk,

- Fiber Patchcord LC-LC SM 3 m – 4 sztuki,

- Twinax SFP-H10GB-CUM3M – 6 sztuk.

* 1. dostarczone urządzenia wraz z podzespołami muszą być fabrycznie nowe, wyprodukowane w 2019 lub 2020 roku, zakupione w oficjalnym kanale sprzedaży producenta. Wraz z dostawą należy dołączyć oświadczenie producenta potwierdzające datę produkcji urządzeń,
  2. urządzenia wraz z podzespołami muszą być dostarczone do Zamawiającego   
     w formie gotowej do uruchomienia bez potrzeby jakichkolwiek czynności   
     po stronie Zamawiającego związanych z montażem/demontażem podzespołów wewnętrznych czy zewnętrznych. Do urządzeń muszą zostać dostarczone wszelkiego rodzaju uchwyty, mocowania, śruby, przewody umożliwiające instalację urządzenia sieciowego w szafie RACK i podłączenia go do sieci elektrycznej i informatycznej Zamawiającego,
  3. prowadzenie prac na infrastrukturze Zamawiającego wymaga spełnienia wymagań procedury dostępu do usług teleinformatycznych Zamawiającego (wypełnienie wniosku) i uzyskanie formalnej zgody Zamawiającego), a także zachowania najwyższej staranności w celu ochrony Infrastruktury Zamawiającego przed możliwym naruszeniem jej bezpieczeństwa,
  4. w przypadku uszkodzenia i konieczności wymiany podzespołów przechowujących trwale zapisane informacje (dyski twarde, pamięci FLASH) Wykonawca pozostawia wymieniane urządzenia u Zamawiającego.
  5. Konfiguracja w siedzibie Zamawiającego (serwerownia OK1), podłączenie   
     i konfiguracja z takim samym urządzeniem zlokalizowanym drugiej lokalizacji (serwerownia w OK2) w klaster HA, konfiguracja podłączenia do sieci Internet, konfiguracja protokołu BGP.

…………………………………………………..

data, imię i nazwisko, podpis osoby uprawnionej