Opis Przedmiotu Zamówienia

## Przedmiot zamówienia

Przedmiotem zamówienia jest rozbudowa posiadanego przez Zamawiającego środowiska „Check Point” o system Checkpoint Maestro wraz z urządzeniami NGFW lub dostarczenie systemu równoważnego.

### W ramach realizacji przedmiotu zamówienia Zamawiający wymaga:

1.1.1 Dostawy urządzeń, akcesoriów, subskrypcji i usług wyspecyfikowanych w tabeli poniżej:

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Nazwa | PN | Ilość |
| 1. | Maestro Hyperscale Orchestrator 175 with 32x 100 GbE ports, plus 1 x 100G DAC (3m) AC power. | CPAP-MHO-175-AC | 4 szt. |
| 2. | Maestro solution with 7000 Security Gateway. | CPAP-SG7000-PLUS-MHS-SNBT | 4 szt. |
| 3. | 40 GbE to four 10 GbE interfaces DAC Splitter, 3m length | CPAC-DAC-40/10G-3M | 4 szt. |
| 4. | MTP/MPO to 4 Duplex LC Breakout Cable, OM3, 3 meter | CPAC-TR-40SPLIT-QSFP-3M | 12 szt. |
| 5. | QSFP+ transceiver for 40G fiber Ports - extended range (40GBase-SR4) - OM3 fiber 300m, OM4 fiber 400m (extended) | CPAC-TR-40SR-QSFP-300m | 16 szt. |
| 6. | 1 CloudGuard Network virtual core for VMware ESXi, Hyper-V, KVM Gateway. Annual subscription for 1 year | CPSG-VSEC-VEN-BUN-NGTP-1Y | 8 szt. |
| 7. | Advanced Technical Account Management. Up to 10 days off site + 2 days on-site | CPTS-PRO-ATAM3-1Y | 1 szt. |
| 8. | Collaborative Enterprise Support – Premium | CPCES-CO-PREMIUM | 1 szt. |
| 9. | Collaborative Enterprise Support - Premium Add-on for Products | CPCES-CO-PREMIUM-ADD | 1 szt. |

1.1.2 Dostarczone licencje / subskrypcje / urządzenia muszą zostać zarejestrowane na koncie Zamawiającego w serwisie producenta pod nr 6289517. – 12 miesięczne wsparcie producenta.

1.1.3 Zamawiający wymaga od Wykonawcy asysty technicznej przy wdrożeniu systemu w wymiarze maksymalnie 20 godzin. Usługa może być wykorzystana przez Zamawiającego w okresie 40 dni roboczych od daty dostarczenia urządzeń, akcesoriów, subskrypcji i usług wyspecyfikowanych w tabeli z punktu 1.1.1.

1.1.4 Asysta wdrożenia odbywać się będzie za pośrednictwem poczty elektronicznej lub telefonicznie przez Zamawiającego, na wskazane dane kontaktowe przez Wykonawcę. Zamawiający wymagać może również zdalnego uczestnictwa asysty technicznej Wykonawcy w spotkaniach za pośrednictwem narzędzi do prowadzenia wideokonferencji będących w posiadaniu Zamawiającego jak również obecności w siedzibie Zamawiającego lub jednej z jednostek (w odległości do 50km od siedziby Zamawiającego).

1.1.5 Zamawiający nie wymaga od wykonawcy wdrożenia systemu.

1.1.6 Oferowane urządzenia wraz z oprogramowaniem muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej są one fabrycznie nowe, kompletne, nieużywane, wyprodukowane nie wcześniej niż w 2021 roku, wolne od wszelkich wad prawnych i fizycznych oraz bez obciążeń i praw osób trzecich, a gwarancja musi pochodzić od producenta i być świadczona przez sieć serwisową producenta, również na terenie Polski.

Gwarancja producenta będzie świadczona w terminie 12 miesięcy od daty dostarczenia.

1.1.7 Miejsce dostawy sprzętu: Dyrekcja Generalna Lasów Państwowych, Warszawa 02-124 ul. Grójecka 127.

### Wymagania dla systemu równoważnego

* + 1. **Wymagania ogólne**
       1. Wszystkie elementy składowe systemu (komponenty) muszą pochodzić od jednego producenta.
       2. Urządzenia muszą być urządzeniami o uznanej na rynku pozycji i muszą znajdować się w kwadracie „Leaders” raportu Gartnera pt. „Magic Quadrant of Network Firewalls” na rok 2020 oraz 2021 lub nowszym
       3. System zapewnia modułową architekturę, umożliwiającą skalowalność oraz wydajność składającą się z oddzielnego tzw. „switching fabric” i grupy wewnętrznych modułów zapory sieciowej dla kontroli ruchu.
       4. System zapewnia, że interfejs „switching fabric” musi umożliwiać połączenie z zewnętrzną infrastrukturą i przeprowadzać równoważenie obciążenia ruchem pomiędzy wewnętrznymi modułami zapory sieciowej.
       5. System zapewnia redundancję sprzętową na poziomie „switching fabric”.
       6. System zapewnia możliwość zwiększenia wydajności, poprzez podłączenie dodatkowych modułów zapory sieciowej do „switching fabric” bez potrzeby rekonfiguracji lub zmian w infrastrukturze L3.
       7. System zapewnia konfigurację active-active pomiędzy modułami zapory sieciowej w ramach jednej fizycznej lokalizacji.
       8. System zapewnia możliwość tworzenia wielu grup klastrowych w ramach rozwiązania, złożonych z modułów zapór sieciowych.
       9. System zapewnia synchronizację stanu sesji między modułami zapory sieciowej w grupie klastrowej.
       10. System zapewnia, że przełączanie awaryjne między modułami zapór sieciowych klastra w grupie, musi odbywać się z zachowaniem stanu sesji.
       11. System zapewnia możliwość dynamicznego przydziału zasobów w postaci modułu zapory sieciowej do grupy klastrowej w czasie rzeczywistym.
       12. System zapewnia redundancję N+1 – utrzymanie wymaganej przepustowości nawet w przypadku awarii jednego z modułu zapory sieciowej.
       13. System zapewnia wsparcie dla tzw. hot-swap modułów zapory sieciowej.
       14. System zapewnia, że dodawanie / usuwanie modułu zapory do/z grupy klastrowej musi odbywać się bez konieczności zmiany ustawień zabezpieczeń i polityki.
       15. System zapewnia możliwość istnienia automatycznego klonowania konfiguracji do nowo dodanych modułów zapory sieciowej.
       16. System zapewnia możliwość centralnego zarządzania grupami klastrowymi.
       17. System zapewnia, że każda grupa klastrowa musi występować jako jeden obiekt z punktu widzenia zarządzania.
       18. System zapewnia, że istnieje obsługa tzw. skalowania w górę/skalowania w dół w odniesieniu do modułów zapór sieciowych.
    2. **Wymagania dotyczące wydajności**
       1. System zapewnia przepustowość dostarczonego rozwiązania, dla pojedynczego modułu zapory sieciowej , o wartości co najmniej 22 Gbps (Enterprise Mix) z możliwością zwiększenia przepustowości, poprzez dodanie modułów zapory sieciowej do trzech razy bez konieczności wymiany sprzętu i zmiany topologii L3.
       2. System zapewnia, przepustowość dostarczonego rozwiązania, z wykorzystaniem Threat Prevention, dla pojedynczego modułu zapory sieciowej, o wartości co najmniej 9,5 Gbps (Enterprise Mix) z możliwością zwiększania przepustowości poprzez dodanie modułów zapory sieciowej do trzech razy bez konieczności wymiany sprzętu i zmiany topologii L3.
       3. System zapewnia zbliżony do liniowego, wzrost wydajności podczas dodawania kolejnego modułu zapory sieciowej do grupy klastrowej (nie więcej niż 10% wpływu na ogólną wydajność).
    3. **Wymagania sprzętowe**
       1. Rozwiązanie powinno zostać dostarczone w postaci appliance’ów, całkowity rozmiar rozwiązania nie może przekraczać 8U.
       2. Rozwiązanie zapewnia montaż w standardowej szafie RACK 19”.
       3. System musi być wyposażony w redundantne zasilacze.
       4. System musi być wyposażony w nadmiarowe moduły wentylatora.
       5. System zapewnia, że każdy interfejs „swiching fabric” musi być wyposażony w 30 interfejsów sieciowych 100 Gbit/s.
       6. System zapewnia, że każdy interfejs „switching fabric” musi być wyposażony w 8 interfejsów sieciowych 10 Gbit/s (dopuszczalne jest wykorzystanie interfejsów 100 Gbit/s i odpowiednich rozdzielaczy interfejsów 100 Gbit/s do 10 Gbit/s).
       7. System zapewnia, że każdy interfejs „switching fabric” musi obsługiwać połączenie modułami zapory sieciowej za pomocą kabli DAC.
       8. System zapewnia dedykowany interfejs zarządzania (port fizyczny).
    4. **Wymagania funkcjonalne**
       1. System musi posiadać predefiniowane zasady IPS.
       2. System musi umożliwiać zdefiniowanie wyjątków IPS zgodnie z kombinacją: SRC IP + DST IP + USŁUGA + ATAK / PODPIS CYFROWY.
       3. System umożliwia przeprowadzanie kontroli reguł zapory na podstawie grup użytkowników z usługi Microsoft Active Directory.
       4. System umożliwia wykrywanie i kontrolowanie aplikacji sieciowych. Liczba wykrywanych aplikacji wynosi co najmniej 8000.
       5. System zapewnia możliwość rozszywania HTTPS.
       6. System zapewnia granularną kontrolę http’s („rozszycie tunelu” lub „baypass”) – zgodnie z kombinacją: SRC IP + NAZWA\_UŻYTKOWNIKA + DST IP + USŁUGA + KATEGORIA APLIKACJI / URL / URL.
       7. System zapewnia ochronę przed znanym złośliwym oprogramowaniem.
       8. System zapewnia blokowanie komunikacji botnetowej na podstawie reputacji, sygnatur i analizy behawioralnej.
       9. System zapewnia ochronę przed nieznanymi zagrożeniami: detonacja plików w środowisku Sandbox, min. Obsługiwane typy plików: powerpoint, word, excel, pdf, exe, archiwa.
       10. System zapewnia możliwość detonacji plików w Sandbox w prywatnej chmurze Zamawiającego Check Point Sandblast.
       11. System zapewnia obsługę VPN client-to-site – zdalny dostęp użytkownika (IPSEC, SSL).
       12. System zapewnia obsługę VPN site-to-site.
       13. System zapewnia konfigurację polityki bezpieczeństwa za pomocą interfejsu GUI. Zdalne połączenie za pomocą protokołów SSH i HTTPS.
    5. **Wymagania dotyczące integracji**
       1. Rozwiązanie musi mieć możliwość integracji z posiadanym przez Zamawiającego systemem zarządzania bezpieczeństwem Check Point SmartCenter (Security Management Server), w szczególności obiekty sieciowe i polityki zdefiniowane w istniejącym systemie zarządzania bezpieczeństwem, muszą mieć możliwość instalacji na każdej z grup klastrowych utworzonych z modułów zapór sieciowych. Instalacja ta musi być możliwa bezpośrednio z konsoli zarządzania Check Point SmartConsole.
    6. **Wymagania dotyczące szkolenia**

W przypadku dostarczenia rozwiązania równoważnego Wykonawca zobowiązuje się do zorganizowania certyfikowanego szkolenia dla 6 osób, obejmującego zarządzanie i administrację dostarczonym oprogramowaniem, szkolenie musi zostać przeprowadzone przez certyfikowana kadrę Producenta oprogramowania. Zakres szkolenia musi pokrywać się tematycznie i być równoważny z autoryzowanymi szkoleniami Check Point CCSA, CCSE i CCME. Szkolenie nie może być krótsze niż   
8 dni roboczych.

Każde szkolenie musi być wykonywane w języku polskim przez trenera dysponującego wiedzą praktyczną i umiejętnościami jej przekazywania. Wykonawca przed rozpoczęciem szkolenia przekaże w formie elektronicznej:

* podręcznik administratora/redaktora,
* szczegółowy plan szkolenia,

Szkolenie musi być potwierdzone stosownym certyfikatem.

W przypadku wprowadzenia na terenie Polski stanu epidemii lub epidemicznego, Zamawiający (po uzgodnieniu z Wykonawcą) dopuszcza przeprowadzenie szkoleń on-line. Szkolenie zdalne musi być przeprowadzone na platformie nie wymagającej zakupienia przez Zamawiającego dodatkowych licencji na specjalne oprogramowanie, a wszelkie koszty związane z zapewnieniem dostępów oraz oprogramowania ponosi Wykonawca. Platforma powinna być wyposażona w funkcjonalność brania w szkoleniu aktywnego udziału przez kursantów tj. powinna być zapewniona możliwość zadawania pytań Wykładowcy. W przypadku konieczności przeprowadzenia szkoleń on-line, Wykonawca prześle Zamawiającemu szczegółowe instrukcje dostępowe do platformy oraz niezbędne oprogramowanie na 7 dni przed przeprowadzeniem szkolenia.