**Załącznik nr 3 do SWZ**

**UKW/DZP-280-D-68/2024**

**FORMULARZ PRZEDMIOTOWO-CENOWY**

* 1. **Urządzenia NGFW – rozbudowa systemu bezpieczeństwa**
  2. **Urządzenie NGFW wraz z obsługą technologii SSL VPN**

**Stan obecny:**

Zamawiający używa obecnie w swojej infrastrukturze systemu bezpieczeństwa opartego o rozwiązania firmy Check Point Software Technologies. System składa się z dwóch urządzeń serii 6600 (CPAP-SG6600-PLUS-SNBT), oraz centralnego systemu zarządzania. Zadaniem systemu bezpieczeństwa jest ochrona zasobów i użytkowników sieci wewnętrznej Zamawiającego, zabezpieczenie dostępu do aplikacji publikowanych przez Zamawiającego w ramach strefy DMZ, a także zapewnienie mechanizmów segmentacji wybranych segmentów sieci wewnętrznej.

System zarządzania ze względu na wolumen logów oparty jest o dwa oddzielne komponenty (serwer zarządzania oraz serwer logów/serwer korelacji zdarzeń) i zaimplementowany został w środowisku wirtualnym Zamawiającego.

Na wszystkie komponenty systemu Zamawiający posiada wsparcie do 27 listopada 2024.

Przedmiotem zamówienia jest rozbudowa opisanego wyżej systemu bezpieczeństwa w celu zabezpieczenia aktualnych i przyszłych potrzeb klienta w zakresie ochrony przed zagrożeniami z sieci Internet. Mechanizmy ochrony przed zagrożeniami powinny uwzględniać minimum kontrolę aplikacji, filtrowanie treści, kontrolę zasobów WWW, ochronę antymalware i antyspyware oraz ochronę przed atakami Zero-day (mechanizm sandboxinu, ochrona przed phishingiem).

**Wymagania ogólne systemu bezpieczeństwa:**

1. Zamawiający wymaga, aby dostarczony system zabezpieczeń był produktem o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) przez co najmniej 36 miesięcy z rzędu.

2. Zamawiający wymaga, aby dostarczone urządzenia były sprzętem zakupionym w oficjalnym kanale sprzedaży producenta na terenie Unii Europejskiej. Zamawiający zastrzega możliwość weryfikacji powyższego wymogu u przedstawiciela producenta oferowanego rozwiązania.

3. Zamawiający wymaga, aby dostarczone urządzenia były nowe oraz pochodziły z bieżącej produkcji. Zamawiający nie dopuszcza dostawy urządzeń, które mogły być używane w innych projektach i zostały poddane procesowi odnowienia.

4. Zamawiający wymaga, aby wszystkie określone w niniejszym dokumencie funkcje systemu były realizowane w aktualnie dostępnych komercyjnie urządzeniach oraz wersjach oprogramowania.

5. Zamawiający wymaga aby elementy systemu zostały dostarczone ze stabilną wersją oprogramowania. Oznacza to, iż rozwiązanie (urządzenia + oprogramowanie) musi być dostępne na rynku nie krócej niż 3 miesiące licząc wstecz od daty ogłoszenia postępowania przetargowego.

6. Zamawiający wymaga, aby wszystkie komponenty systemu bezpieczeństwa zainstalowane zostały lokalnie w ramach infrastruktury Zamawiającego.

7. Zamawiający wymaga, aby wszystkie komponenty programowe oraz urządzenia wchodzące w skład systemu bezpieczeństwa pochodziły od jednego producenta.

8. Wraz z dostawą systemu/oprogramowania i urządzeń Wykonawca dostarczy:

1. dokument potwierdzający, że oprogramowanie w nim zawarte jest licencjonowane na Zamawiającego,
2. dokument potwierdzający zarejestrowanie kontraktu i dokument potwierdzający dostęp Zamawiającego do bazy wiedzy, do najnowszych wersji oprogramowania i jego aktualizacji, poprawek, zgłoszeń dotyczących awarii, usterek oprogramowania i wsparcia technicznego i dokumentacji, w ramach stron WWW Producenta, dostępnych po zalogowaniu na indywidualne konto Zamawiającego,
3. szczegółową dokumentację techniczną producenta oferowanych urządzeń, potwierdzającą spełnianie wymagań technicznych urządzeń będących przedmiotem zamówienia.

**Rozbudowa systemu bezpieczeństwa:**

Rozbudowa systemu złożona jest z dwóch elementów – odnowienia wymaganych licencji i wsparcia producenta dla komponentów warstwy zarządzania oraz dostarczenia nowego, wydajniejszego komponentu który docelowo przejmie rolę klastra urządzeń Check Point serii 6600.

Tabela nr 1 zawiera wykaz wykorzystywanych aktualnie komponentów systemu bezpieczeństwa, które wymagają odnowienia wsparcia producenta. Zamawiający wymaga odnowienia wymienionych produktów na okres 36 miesięcy.

|  |  |  |  |
| --- | --- | --- | --- |
| Nazwa produktu | SKU | CK lub S/N | Konto UC |
| Next Generation Security Management Software for 5 gateways (SmartEvent & Compliance 1 year) | CPSM-NGSM5 | CFBB0F0E8B66 | 8118961 |
| Next Generation Security Management SmartEvent dedicated Server for 5 gateways (perpetual) | CPSM-NGSM5-EVNT | 6B9564E8C00C | 8118961 |

Poniższa tabela nr 2 zawiera wykaz nowych, wymaganych przez Zamawiającego komponentów systemu które powinny zostać dostarczone wraz ze wszystkimi wymaganymi licencjami i oprogramowaniem.

|  |  |  |
| --- | --- | --- |
| Produkt | SKU | Ilość |
| 9400 Plus Appliance with 2 Virtual Systems and SandBlast subscription package for 1 year | CPAP-SG9400-PLUS-SNBT | 2 |
| Next Generation Threat Prevention and Sandblast for additional 2 years for 9400 PLUS Appliance | CPSB-SNBT-9400-PLUS-2Y | 2 |
| SFP+ transceiver for 10G Fiber Ports- short range (10GBase-SR)- for 9000/19000/29000 appliances | CPAC-TR-10SR-D | 24 |
| 32GB Memory upgrade kit for 9100-9400 appliances | CPAC-RAM32GB-9100/9400-INSTALL | 2 |
|  |  |  |

Zamawiający dopuszcza składanie ofert równoważnych w rozumieniu art. 99 ust. 5 ustawy Pzp. W przypadku zaoferowania rozwiązania równoważnego na Wykonawcy spoczywa obowiązek wykazania jego równoważności.

Zastosowanie rozwiązania równoważnego nie będzie wymagało żadnych nakładów po stronie Zamawiającego celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury.

Zamawiający dopuszcza dostarczenie przez Wykonawcę urządzeń równoważnych spełniających poniższe wymagania:

**1) Urządzenia NGFW – rozbudowa systemu bezpieczeństwa**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametry oferowane (proszę wypełnić dokładnie niniejszy opis oraz podać producenta oraz typ/model oferowanego urządzenia wraz z nazwą, typem/modelem poszczególnych podzespołów składowych np. procesora, zasilaczy, wentylatora itp.)** | **Liczba szt.** | **Cena jednostkowa netto** | **Wartość**  **netto** | **%VAT** | **Wartość brutto** |
| **1A) Urządzenie NGFW - 2 sztuki (system HA)** | |  | 1 komplet (dwa fizyczne urządzenia) |  |  |  |  |
| **Producent** | należy wskazać -> |  |  | | | | |
| **Typ/Model** | należy wskazać -> |  |
| **OPIS** | 1. Wszystkie wymagane funkcjonalności muszą być dostępne w dniu składania oferty.  2. Wszystkie komponenty systemu zabezpieczeń (zwany również systemem NGFW) muszą pochodzić o tego samego producenta i muszą zostać zainstalowane w ramach infrastruktury Zamawiającego.  3. Zarządzanie politykami bezpieczeństwa implementowanymi w systemie NGFW musi odbywać się centralnie z poziomu centralnego serwera zarządzania i raportowania (CSZiR)  4. W ramach postępowania muszą zostać dostarczone dwa kompletne, gotowe do pracy urządzenia skonfigurowane w trybie HA (ang. High Availability).  5. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta.  6. System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.  7. Interfejsy sieciowe systemu NGFW muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (monitoring).  8. Konfiguracja trybu pracy interfejsów sieciowych systemu NGFW musi być ustalana w konfiguracji interfejsu sieciowego, a system NGFW musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).  9. System NGFW musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q z obsługą do 1024 znaczników VLAN w trybie Gateway oraz 4096 znaczników w trybie wirtualnych systemów.  10. System NGFW musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP, OSPF (v2 oraz v3).  11. System NGFW musi realizować inspekcję stanową opartą na granularnej analizie komunikacji oraz stanu aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu  12. Polityka zabezpieczeń systemu NGFW musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzania pasmem.  13. System NGFW musi pozwalać na konfiguracje reguł polityki bezpieczeństwa z uwzględnieniem okresu czasu w jakim dana reguła będzie aktywna (egzekwowana). Definicja okresu czasu, w ramach którego dana reguła jest aktywna powinna uwzględniać następujące parametry: data i/lub godzina startu, data i/lub godziny zakończenia oraz rekurencyjność.  14. System NGFW musi mieć możliwość automatycznego pobierania, z zewnętrznych serwerów, list z adresami IP i/lub Domenami. Pobranie powinno następować automatycznie i tylko wtedy, gdy treść zewnętrznej listy zostanie zaktualizowana. Funkcjonalność ta musi mieć również możliwość uwierzytelnienia połączenia do zewnętrznego serwera oraz możliwość użycia serwera proxy w celu pobrania listy.  15. System NGFW musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników - integracja z Active Directory. Polityka kontroli dostępu (firewall) powinna precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci.  16. System NGFW musi domyślnie działać zgodnie z zasadą blokowania całego ruchu sieciowego, poza tym który jest zdefiniowany w regułach polityk bezpieczeństwa i wskazany jako dozwolony  17. System NGFW musi wykonywać 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.  18. System NGFW musi być wyposażony w moduł IPS, który pracuje w trybie in-line. Moduł IPS musi posiadać możliwość konfiguracji w trybie pasywnym (Detect) lub w trybie Prevent (aktywne blokowanie niebezpiecznych połączeń).  19. Moduł IPS musi dokonywać inspekcji całych sesji/połączeń. Nie dopuszcza się rozwiązań określających bezpieczeństwo sesji poprzez szczątkową analizę ruchu podczas ustanawiania sesji.  20. Moduł IPS musi zapewniać ochronę co najmniej z wykorzystaniem sygnatur ataków oraz mechanizmu wykrywania anomalii w protokołach.  21. Moduł IPS musi mieć możliwość zapisywania pakietów generujących incydenty bezpieczeństwa.  22. Moduł IPS musi posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji  23. Moduł IPS musi zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera aktualizacji w sposób uniemożliwiający ich modyfikację podczas przesyłania pomiędzy serwerem aktualizacji oraz serwerem zarządzania/zaporą sieciową.  24. Moduł IPS musi zapewniać mechanizm zarządzania wersjami bazy sygnatur oraz umożliwiać powrót do wybranej wersji.  25. Moduł IPS musi zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednoczenie.  26. Moduł IPS musi zapewniać możliwość obsługi reguł Snort  27. Moduł IPS musi pozwalać posiadać możliwość aktywowania ochrony dla wybranych zasobów definiowanych minimum w postaci adresów hostów, adresów sieci oraz zakresów adresów IP i przypisywanie do tych zasobów dedykowanych zestawów sygnatur.  28. Moduł IPS musi posiadać mechanizmy wykrywania i blokowania operacji tunelowania ruchu w ramach innych protokołów, np. DNS tunneling  29. System NGFW musi być wyposażony w moduł kontroli aplikacji, który pozwala na identyfikację minimum 6000 różnych aplikacji.  30. Moduł kontroli aplikacji musi posiadać mechanizm ograniczenia użycia pasma dla poszczególnych aplikacji niezależnie dla każdego kierunku przepływu danych (download oraz upload)  31. Moduł kontroli aplikacji musi posiadać możliwość współpracy z modułem analizy treści w zakresie wykrywania i blokowania przesyłania określonych typów danych (np.nr kart kredytowych) oraz określonych typów plików (np. csv, pdf i inne) w ramach zidentyfikowanej aplikacji. W przypadku, kiedy opisany mechanizm wymaga dodatkowej licencji to powinna ona zostać dostarczona razem z systemem bezpieczeństwa.  32. Moduł kontroli aplikacji musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do aplikacji, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej aplikacji.  33. Moduł kontroli aplikacji musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowanie użytkowników do stron umieszczonych na zewnętrznych serwerach.  34. System NGFW musi umożliwiać administratorom rozszerzenie wbudowanej bazy aplikacji poprzez samodzielne tworzenie nowych sygnatur aplikacji. Jeżeli funkcjonalność ta wymaga dodatkowej licencji to stosowna licencja powinna być dostarczone razem z systemem.  35. Moduł kontroli aplikacji musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania.  36. System NGFW musi zapewniać mechanizmy inspekcji komunikacji szyfrowanej HTTPS oraz inspekcji komunikacji realizowanej w oparciu o protokół SSH. w ramach inspekcji ruchu HTTPS system NGFW musi wspierać protokoły TLS 1.2 oraz TLS 1.3  37. System NGFW musi pozwalać na inspekcję ruchu HTTPS zarówno dla ruchu wychodzącego z sieci organizacji (np. komunikacja użytkowników z usługami w sieci Internet) jaki i ruchu przychodzącego kierowanego do usług udostępnianych przez organizację. Inspekcja powinna obejmować analizę ruchu pod kątem zgodności z regułami polityki dostępowej (np. kontrola aplikacji oraz kategorii URL) oraz weryfikować ruch pod kątem ewentualnych zagrożeń (np. moduł IPS, moduł antywirusowy).  38. System NGFW musi umożliwiać administratorom zdefiniowanie reguł określających jaka część ruchu HTTPS ma zostać poddana inspekcji, a jaka ma zostać z niej wykluczona. W ramach definiowania reguł administrator musi posiadać możliwość określenia jakie mechanizmy inspekcyjne (moduły) mają zostać wykorzystane podczas analizy ruchu (np. ochrona antywirusowa).  39. System NGFW musi umożliwiać utworzenie więcej niż jednego zbioru reguł określających zakres ruchu HTTPS podlegający inspekcji. System musi umożliwiać przypisywanie zbiorów reguł do określonych polityk bezpieczeństwa, a także współdzielenie określonych zbiorów reguł przez więcej niż jedną politykę bezpieczeństwa.  40. W ramach mechanizmu inspekcji wychodzącego ruchu HTTPS system NGFW musi umożliwiać weryfikację stanu certyfikatu cyfrowego serwera docelowego. System musi umożliwiać blokowanie ruchu do określonego serwera docelowego w przypadku kiedy jego certyfikat został unieważniony, wygasł lub nie został podpisany przez zaufany urząd certyfikacji.  41. System NGFW musi umożliwiać tworzenie listy niezaufanych certyfikatów cyfrowych i w efekcie pozwalać na blokowanie ruchu kierowanego do serwerów, które takie certyfikaty wykorzystują.  42. System NGFW musi umożliwiać wysyłanie kopii odszyfrowanego ruchu HTTPS na wskazany interfejs urządzenia w celu zasilania zewnętrznych systemów bezpieczeństwa.  43. System NGFW musi zapewniać mechanizmy pozwalające na inspekcję szyfrowanej komunikacji SSH. Niedopuszczalne jest aby system do deszyfracji SSH używał jednego globalnego klucza deszyfrującego  44. W ramach inspekcji ruchu SSH system NGFW musi zapewniać możliwość analizy ruchu przy pomocy modułu wykrywania włamań (IPS) oraz umożliwiać analizę przesyłanych plików minimum przy pomocy modułu antywirusowego.  45. System NGFW musi być wyposażony w moduł filtrowania kategorii URL  46. Moduł filtrowania kategorii URL musi posiadać możliwość tworzenia reguł polityki zawierających jednocześnie wiele kategorii URL.  47. Moduł filtrowania kategorii URL musi dostarczać wbudowane kategorie URL opisujące niebezpieczne witryny kategoryzowane w oparciu o poziom zagrożenia (np. CriticalRisk lub High Risk), a także w oparciu o rodzaj zagrożenia (np. witryny wyłudzające dane lub witryny będące centrami C&C)  48. Moduł filtrowania kategorii URL musi umożliwiać tworzenie własnych obiektów opisujących witryny URL oraz ich kategoryzowanie.  49. Moduł filtrowania kategorii URL musi umożliwiać tworzenie obiektów należących do więcej niż jednej kategorii URL.  50. Moduł filtrowania kategorii URL musi umożliwiać lokalne nadpisywanie domyślnej kategorii URL dla wybranych witryn.  51. Moduł filtrowania kategorii URL musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do określonej witryny, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej witryny.  52. Moduł filtrowania kategorii URL musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowania użytkowników do stron umieszczonych na zewnętrznych serwerach.  53. System NGFW musi być wyposażony w moduł ochrony antywirusowej oraz moduł zabezpieczający przed próbami komunikacji z sieciami botnet.  54. System zapobiegania komunikacji z sieciami botnet musi umożliwiać wykrycie oraz zablokowanie podejrzanego zachowania w chronionych segmentach sieci  55. System zapobiegania komunikacji z sieciami botnet w celu identyfikacji podejrzanych zachowań musi wykorzystywać mechanizmy zabezpieczeń oparte o reputację adresów IP, URL oraz DNS w połączeniu z wykrywaniem wzorców ruchu specyficznych dla połączeń kierowanych do serwerów C&C.  56. System zapobiegania komunikacji z sieciami botnet musi posiadać możliwość identyfikacji urządzeń wewnętrznych będących źródłem podejrzanych zapytań DNS w przypadku kiedy wykorzystują one wewnętrzny serwer DNS pośredniczący w generowaniu zapytań. Mechanizm musi umożliwiać modyfikację/fałszowanie odpowiedzi DNS i przekierowywanie urządzeń do wcześniej ustalonego adresu IP (tzw. DNS malware trap lub DNS Sinkhole).  57. Moduł ochrony antywirusowej musi zapewniać ochronę minimum dla następujących protokołów: HTTP/HTTPS, FTP, SMB/CIFS (w tym SMBv3)  58. Moduł ochrony antywirusowej musi umożliwiać skanowanie plików skompresowanych. Administrator musi mieć możliwość zdefiniowania maksymalnego czasu skanowania pojedynczego archiwum oraz zdefiniowania akcji (przekaż lub zablokuj) która zostanie podjęta w momencie przekroczenia zdefiniowanego limitu.  59. Moduł ochrony antywirusowej musi posiadać możliwość blokowania dostępu do określonych witryn internetowych w oparciu o informację o ich reputacji.  60. Moduły ochrony antywirusowej oraz zapobiegania komunikacji z sieciami botnet muszą posiadać możliwość interakcji z użytkownikami w zakresie informowania o zablokowaniu dostępu do niebezpiecznych zasobów.  61. System bezpieczeństwa musi umożliwiać rozszerzenie bazy informacji o zagrożeniach poprzez dodawanie zewnętrznych definicji IoC (Indicator of Compromise) w formacie pliku CSV lub STIX XML (STIX 1.0).  62. System NGFW musi być wyposażony w moduł ochrony przed atakami 0-day (sandboxing, CDR). System NGFW musi umożliwiać przesyłanie podejrzanych plików do analizy systemie sandboxingowym. Jeżeli opisana funkcjonalność wymaga dodatkowej licencji to licencja powinna być dostarczona razem z systemem NGFW.  63. Moduł ochrony przed atakami 0-day musi umożliwiać otwarcie dostarczonego za pośrednictwem wspieranych protokołów pliku w wirtualnym systemie operacyjnym, analizę skutków otwarcia pliku w tym systemie a następnie podjęcie akcji (zablokuj/przekaż do odbiorcy) w zależności od uzyskanych wyników analizy. Szczegółowy wynik analizy powinien zostać udokumentowany w formie raportu i przesłany na wskazany serwer logów.  64. Niedopuszczalne jest aby moduł ochrony przed atakami 0-day przekazał analizowany plik do odbiorcy przed uzyskaniem wyniku z procesu analizy w środowisku wirtualnym potwierdzającego że analizowany plik jest bezpieczny. Wyjątkiem jest dostarczenie do użytkownika bezpiecznej wersji pliku, tzn. wersji pozbawionej całej treści aktywnej. Jako treść aktywna rozumiane są między innymi makra pakietu MS Office, odnośniki do zewnętrznych zasobów, obrazy, kwerendy do baz danych, skrypty JavaScript, filmy i inne.  65. Moduł ochrony przed atakami 0-day musi umożliwiać wykonywanie analizy zachowania plików w środowiskach wirtualnych opartych o różne wersje systemu operacyjnego Microsoft Windows oraz różne pakiety oprogramowania Microsoft Office. Licencja dostarczona wraz z modułem musi zawierać prawa do użytkowania zewnętrznego oprogramowania zawartego w obrazach systemów do celów analizy plików w środowiskach wirtualnych.  66. System NGFW musi być wyposażony w moduł do realizacji bezpiecznych połączeń zdalnych.  67. Moduł do realizacji bezpiecznych połączeń zdalnych musi umożliwiać nawiązywanie połączeń w trybie punkt-punkt (site-to-site) oraz zapewniać możliwość dostępu do zasobów dla użytkowników zdalnych (remote access)  68. Moduł do realizacji bezpiecznych połączeń zdalnych musi umożliwiać nawiązywanie połączeń w oparciu o protokół IKEv1 oraz IKEv2  69. Moduł do realizacji bezpiecznych połączeń zdalnych musi umożliwiać nawiązywanie połączeń w następujących topologiach: full mesh, star, hub-and-spoke  70. Moduł do realizacji bezpiecznych połączeń zdalnych musi umożliwiać kreowanie tuneli w oparciu o klucz współdzielony (preshared key) oraz certyfikaty cyfrowe. W przypadku certyfikatów cyfrowych musi istnieć możliwość wykorzystania certyfikatów wystawianych przez wewnętrzny urząd certyfikacji wbudowany w produkt lub przez zewnętrzne urzędy certyfikacji  71. Moduł do realizacji bezpiecznych połączeń zdalnych musi umożliwiać uruchomienie mechanizmu split-tunneling dla połączeń od użytkowników zdalnych.  72. Moduł do realizacji bezpiecznych połączeń zdalnych musi zapewniać możliwość zestawienia minimum 3000 jednoczesnych połączeń od użytkowników zdalnych.  73. Niedopuszczalne jest aby do realizacji bezpiecznych połączeń zdalnych ograniczał licencyjnie liczbę tuneli punkt-punkt jakie mogą zostać nawiązane z poziomu zapory sieciowej.  74. System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance) przystosowane do instalacji w szafach rack 19 cali.  75. Urządzenia pełniące rolę zapory sieciowej muszą być wyposażone w pamięć DRAM nie mniejszą niż 64GB.  76. Urządzenia pełniące rolę zapory sieciowej muszą być wyposażone w dysk SSD o pojemności nie mniejszej niż 960GB.  77. W komplecie muszą znajdować się szyny umożliwiające montaż urządzenia w szafie rack oraz kable zasilające, zaślepki na miejsca dla nieużywanych modułów itp.  78. Każde z urządzeń w klastrze HA musi być wyposażone w co najmniej jeden port konsoli oraz w co najmniej jeden dedykowany port zarządzający.  79. System musi być wyposażony w co najmniej 1 dedykowany port na potrzeby HA.  80. Każde z urządzeń w klastrze HA musi posiadać przepływność w ruchu full-duplex nie mniej niż 33 Gbit/s dla kontroli firewall z włączoną funkcją IPS oraz kontrolą aplikacji oraz nie mniej niż 11 Gbit/s dla kontroli zawartości (moduły firewall, kontrola aplikacji, kategoryzacja URL, moduł antywirusowy, IPS, ochrona Zero-Day)  81. Każde z urządzeń w klastrze HA musi obsługiwać nie mniej niż 16 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 355 000 połączeń na sekundę.  82. Każde z urządzeń w klastrze HA musi posiadać co najmniej 2 redundantne zasilacze umożliwiające podłączenie urządzenia do sieci energetycznej 230V.  83. Każde z urządzeń w klastrze HA musi być wyposażone w co najmniej następujące interfejsy sieciowe:  a. 8 portów 1Gbps RJ45, przeznaczone do ruchu produkcyjnego.  b. 12 portów 1/10Gbps SFP+ obsadzone wkładkami 1/10G SR, przeznaczone do ruchu produkcyjnego. Zamawiający wymaga dostarczenia również 10 wkładek 10Gbase-SR, kompatybilnych z posiadanym w zasobach Zamawiającego modułem sieciowym dla C6500: WS-X6708-10GE. Moduły te, nie muszą pochodzić od tego samego producenta, co posiadane rozwiązanie oraz oferowane urządzenia NGFW.  84. System NGFW musi zostać dostarczony z wraz z kompletem wymaganych licencji do uruchomienia opisanych wyżej mechanizmów ochronnych na okres 36 miesięcy. |  |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametry oferowane (proszę wypełnić dokładnie niniejszy opis oraz podać producenta oraz typ/model oferowanego urządzenia wraz z nazwą, typem/modelem poszczególnych podzespołów składowych np. procesora, zasilaczy, wentylatora itp.)** | **Liczba szt.** | **Cena jednostkowa netto** | **Wartość**  **netto** | **%VAT** | **Wartość brutto** |
| **1B) Centralny System Zarządzania i Raportowania (w skrócie CSZiR) – dla oferowanych powyżej rozwiązań NGFW** | |  | 1 komplet (management + event system) |  |  |  |  |
| **Producent** | należy wskazać -> |  |  | | | | |
| **Typ/Model** | należy wskazać -> |  |
| **OPIS** | 1. Zamawiający posiada centralny system zarządzania firmy Check Point złożony z komponentów Next Generation Security Management Software for 5 Gateways (CPSM-NGSM5) oraz Next Generation Security Management SmartEvent dedicated Server for 5 gateways (CPSM-NGSM5-EVNT), który udostępni Wykonawcy do wykorzystania w celu zbudowania systemu zarzadzania i raportowania.  W przypadku wykorzystania tych urządzeń Wykonawca zobowiązuje się do objęcia ich wsparciem producenta na okres 36 miesięcy.  2. W przypadku jeżeli Wykonawca nie wykorzysta udostępnionych w pkt. 1 urządzeń jest zobowiązany dostarczyć wraz z urządzeniami NGFW:  a. oprogramowanie zarządzania i raportowania przystosowane do współpracy z dostarczonymi urządzeniami NGFW  b. Zamawiający wymaga aby wszystkie komponenty CSZiR zostały zainstalowane w lokalnie w środowisku Zamawiającego  c. w ramach CSZiR Zamawiający wymaga minimum następujących funkcjonalności:  i. centralne zarządzanie polityką bezpieczeństwa (w zakresie polityki dostępowej oraz ochrony przed zagrożeniami) na wszystkich zarządzanych urządzeniach NGFW  ii. funkcja serwera logów pozwalająca na centralne przechowywanie oraz indeksowanie logów pochodzących z zarządzanych urządzeń NGFW  iii. funkcja korelacji oraz wykrywania incydentów bezpieczeństwa – wykrywanie oraz raportowanie incydentów bezpieczeństwa na bazie logów pochodzących z zarządzanych urządzeń  iv. moduł raportowania  d. Zamawiający dopuszcza realizację funkcjonalności CSZiR opisanych punkcie 2c przy zastosowaniu platformy sprzętowej lub wirtualnej (wymagane wsparcie dla instalacji w środowisku VMWare) . Każda platforma, niezależnie od typu, powinna zapewniać minimalnie 2TB powierzchni dyskowej oraz umożliwiać zapis minimum 7GB logów dziennie.  e. Zamawiający dopuszcza realizację funkcjonalności CSZiR opisanych w punkcie 2c przez więcej niż jedną maszynę wirtualną lub fizyczną, jeżeli taka potrzeba wynika z architektury oferowanego rozwiązania.  f. Zamawiający wymaga aby CSZiR był obsługiwany za pomocą konsoli użytkownika, która ma być dostarczona w postaci graficznej konsoli administratora (GUI) działającej pod systemem operacyjnym Windows. Konsola zarządzania powinna posiadać możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.  g. Zamawiający wymaga aby komunikacja CSZiR pomiędzy modułem zapory sieciowej (funkcjonujących na zewnętrznych urządzeniach) i modułem zarządzania i raportowania (CSZiR) powinna być szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych generowanych przez moduł zarządzania i raportowania (CSZiR).  h. Zamawiający wymaga aby komunikacja pomiędzy interfejsem GUI i CSZiR była szyfrowana  i. Zamawiający wymaga aby CSZiR zapewniał możliwość uwierzytelnianie administratorów za pomocą haseł statycznych, haseł dynamicznych, certyfikatów cyfrowych oraz protokołu SAML.  j. Zamawiający wymaga aby CSZiR zapewniał możliwość definiowania szczegółowych zestawów uprawnień dla poszczególnych administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników)  k. Zamawiający wymaga aby CSZiR umożliwiał jednoczesną pracę wielu administratorów - w tym także jednoczesną pracę w ramach pojedynczej polityki bezpieczeństwa.  l. Zamawiający wymaga aby CSZiR posiadał mechanizm wieloetapowej akceptacji zmian wykonanych w polityce bezpieczeństwa przez minimum dwóch różnych administratorów. Jeżeli opisana funkcjonalność wymaga dodatkowej licencji to powinna być ona dostarczona razem z CSZiR.  m. Zamawiający wymaga aby CSZiR zapewniał możliwość tworzenia wielu różnych polityk bezpieczeństwa oraz umożliwiać ich przypisanie do zarządzanych urządzeń NGFW.  n. Zamawiający wymaga aby CSZiR posiadał mechanizmy automatycznej weryfikacji spójności i niesprzeczności implementowanej polityki bezpieczeństwa przed zainstalowaniem jej na urządzeniach NGFW.  o. Zamawiający wymaga aby CSZiR posiadał wbudowane mechanizmy wersjonowania polityk bezpieczeństwa. Nowa wersja polityki bezpieczeństwa powinna być tworzona każdorazowo w momencie opublikowania zmian przez administratora systemu. System wersjonowania musi zapewniać administratorom możliwość wglądu w wybraną wersję polityki bezpieczeństwa, możliwość porównywania różnych wersji polityki pod kątem różnic między nimi, a także opcję cofnięcia konfiguracji do wybranej wersji.  p. Zamawiający wymaga aby CSZiR posiadał mechanizmy zapewniające rozliczalność zmian konfiguracyjnych wykonanych przez poszczególnych administratorów w formie generowania i przechowywania logów audytowych. Logi muszą zawierając minimum informacje o tożsamości administratora oraz czasie i zakresie wykonywanych zmian  q. Zamawiający wymaga aby CSZiR posiadał mechanizmy centralnego zarządzania licencjami dla wszystkich komponentów wchodzących w skład systemu bezpieczeństwa.  r. Zamawiający wymaga aby CSZiR posiadał dedykowane API umożliwiające automatyzację czynności administracyjnych.  s. Zamawiający wymaga aby CSZiR realizował funkcję serwera logów w ramach której musi umożliwiać agregację i indeksowanie logów ze wszystkich zarządzanych urządzeń NGFW. W ramach funkcji serwera logów muszą istnieć wbudowane mechanizmy ochrony przestrzeni dyskowej przed przepełnieniem  t. Zamawiający wymaga aby CSZiR posiadał mechanizmy pozwalające na implementację rozwiązania wysokiej dostępności, w ramach której możliwe jest dodanie zapasowego serwera zarządzania oraz uruchomienie automatycznej synchronizacji konfiguracji polityk bezpieczeństwa. Dostarczenie zapasowego serwera zarządzania nie jest wymagane w ramach postępowania.  u. Zamawiający wymaga aby CSZiR posiadał możliwość wykrywania incydentów bezpieczeństwa na bazie logów pochodzących z zarządzanych urządzeń NGFW.  v. Zamawiający wymaga aby CSZiR pozwalał na wyszukiwanie wymaganych informacji (logów, incydentów bezpieczeństwa) zapisanych w wewnętrznej bazie danych bez konieczności definiowania wartości dla poszczególnych atrybutów (tzw.freetext search).  w. Zamawiający wymaga aby CSZiR posiadał funkcję pozwalającą na grupowanie wyników wyszukiwania logów/incydentów bezpieczeństwa według określonych atrybutów (minimum typ incydentu, zasoby, nazwa użytkownika).  x. Zamawiający wymaga aby CSZiR umożliwiał administratorom tworzenie własnych raportów oraz ekranów (dashboard), a także modyfikowanie raportów i widoków dostarczonych razem z systemem.  y. Zamawiający wymaga aby CSZiR posiadał możliwość konfigurowania automatycznych reakcji na wykryte incydenty bezpieczeństwa - minimum w postaci wysłania wiadomość e-mail, wygenerowanie SNMP trap lub uruchomienie skryptu  z. Zamawiający wymaga dostarczenie odpowiednich subskrypcji, gwarancji producenta i licencji dla w/w rozwiązania na okres 36 miesięcy. |  |
|  |  |  |

**2) Urządzenie NGFW wraz z obsługą technologii SSL VPN**

**Ważna informacja:**

Zamawiający posiada wdrożone rozwiązanie, w oparciu o technologię Cisco SecureClient (AnyConnect). Nie przewiduje tym samym realizacji projektu, polegającego na wymianie technologii VPN, w tym klientów VPN, dla kilku tysięcy użytkowników.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametry oferowane (proszę wypełnić dokładnie niniejszy opis oraz podać producenta oraz typ/model oferowanego urządzenia wraz z nazwą, typem/modelem poszczególnych podzespołów składowych np. procesora, zasilaczy, wentylatora itp.)** | **Liczba szt.** | **Cena jednostkowa netto** | **Wartość**  **netto** | **%VAT** | **Wartość brutto** |
| **Urządzenie NGFW wraz z obsługą technologii SSL VPN** | |  | 1 |  |  |  |  |
| **Producent** | należy wskazać -> |  |  | | | | |
| **Typ/Model** | należy wskazać -> |  |
| **OPIS** | 1. Urządzenie musi być będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia  2. Urządzenie musi być wyposażone w porty minimum:  a) 8x 1GE RJ45  b) 8x 1/10GE SFP+  3. Urządzenie musi być wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band  4. Urządzenie musi być wyposażone w port USB 3.0  5. Urządzenie musi być wyposażone w dysk twardy o pojemności minimum 800GB  6. Urządzenie musi być zasilanie prądem przemiennym 230V  7. Urządzenie musi być wyposażone w redundantny zasilacz, zasilacze mogą być wymieniane podczas pracy urządzenia („na gorąco”).  8. Urządzenie musi być wyposażone w elementy do montażu w szafie rack 19” (komponenty te muszą wchodzić w skład zestawu)  9. Wysokość urządzenia: 1RU  10. Urządzenie musi być objęte 3-letnim serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.  11. Zamawiający wymaga dostarczenia licencji na połączenia zdalne VPN (w tym SSL VPN) dla 5000 jednoczesnych użytkowników, możliwych do wykorzystywania przez okres minimum 3 lat, dla urządzeń mobilnych oraz komputerów stacjonarnych.  12. Przepustowość urządzenia dla uruchomionych modułów firewall’a oraz kontroli aplikacji na poziomie minimum 21Gbps dla pakietów wielkości 1024B.  13. 4 000 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 170 000 nowych połączeń na sekundę.  14. Możliwość połączenia VPN do 7 000 urządzeń, z sumaryczną przepustowością minimum 10Gbps dla pakietów 1024B TCP.  15. Przepustowość dekrypcji ruchu szyfrowanego przynajmniej 6,7Gbps.  16. Urządzenie musi obsługiwać interfejsy VLAN (802.1Q) na interfejsach fizycznych – 1000 interfejsów VLAN.  17. Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.  18. Możliwość uruchomienia urządzenia w trybie firewall’a L3, jak i w trybie transparentnym  19. Urządzenie musi obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP).  20. Urządzenie musi posiadać możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory  21. Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT oraz PAT)  22. Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standby  23. Urządzanie musi zapewniać możliwość obsługi użytkowników zdalnych VPN (RA VPN)  24. Urządzenie zapewnia funkcjonalności:  a) systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control)  b) systemu IPS  c) systemu ochrony przed malware  d) systemu filtracji ruchu w oparciu o URL  Jeśli którakolwiek funkcjonalność, o których mowa jest w punkcie 24, wymaga dodatkowej licencji, Zamawiający nie wymaga jej dostarczenia.  25. Urządzenie musi posiadać 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:  a) Wiedza o użytkownikach – uwierzytelnienie  b) Wiedza o urządzeniach – pasywne skanowanie ruchu  c) Wiedza o urządzeniach mobilnych  d) Wiedza o aplikacjach wykorzystywanych po stronie klienta  e) Wiedza o podatnościach  f) Wiedza o bieżących zagrożeniach  g) Baza danych URL  26. Urządzenie musi posiadać otwarte API dla współpracy z systemami zewnętrznym  27. Urządzenie musi posiadać możliwość wykrywania aplikacji zapewniający:  a) możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji  b) możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług  c) wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji  d) współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach |  |

**Dotyczy pozycji 1 oraz 2:**

* Zamawiający wymaga udzielenie licencji, wsparcia, serwisu i gwarancji na co najmniej 3-letni okres (z możliwością przedłużenia o co najmniej kolejne dwa lata). Dla pozycji nr 1 dopuszcza się świadczenie usługi serwisu, wsparcia i gwarancji poprzez Partnera Producenta, jeżeli Producent rozwiązania dopuszcza taką możliwość. Reżim gwarancyjny, zgodnie z oficjalną polityką Producenta, świadczony w trybie NBD 8x5.
* Sprzęt musi być nowy, wolny od wad i pochodzić z legalnego (względem oficjalnej polityki Producenta) kanału dystrybucji oraz aktualnej oferty producenta.
* Zamawiający wymaga, aby Oferent wskazał w formularzu cenowym sposób licencjonowania (licencja ograniczona czasowo / wieczysta) zaoferowanych komponentów / funkcjonalności wchodzących w skład oferowanego rozwiązania.
* Zamawiający wymaga dostarczenia w/w produktów wraz z usługą wsparcia wdrożeniowego (z opisanymi poniżej elementami wdrożenia) i powdrożeniowego świadczonego przez Dostawcę (40 godzin biznesowych [pn-pt w godz. 08:00 – 16:00], do wykorzystania w ciągu roku kalendarzowego od dnia podpisania przez Strony umowy). Usługa konsultacyjna świadczona zdalnie, za pomocą środków elektronicznych (np. interaktywnych komunikatorów on-line, telefonu lub poczty e-mail) lub w siedzibie Wykonawcy, polegać będzie na asyście personelowi UKW, podczas wdrażania zamawianych produktów, ich integracji wzajemnej oraz integracji z będącym w zasobach Zamawiającego system bezpieczeństwa, o którym mowa jest w tym dokumencie (on-line lub na miejscu, po wcześniejszym uzgodnieniu tego faktu przez Strony, w trybie operacyjnym: mail, telefon - przewiduje się co najmniej 80% świadczenia tej usługi w trybie zdalnym) oraz jego utrzymania w środowisku produkcyjnym, w zakresie czasowym do jednego roku kalendarzowego od podpisania przez Strony umowy. **Czas reakcji Wykonawcy na zgłoszenie w zakresie wsparcia Zamawiającego** (e-mail, telefon lub dedykowany portal WWW Wykonawcy): najpóźniej next business day (NBD). Wykonawca zobowiązuje się również wspierać Zamawiającego, jeżeli zajdzie konieczność zarejestrowania zgłoszenia przez Zamawiającego w portalu Producenta lub złoży takie zgłoszenie w imieniu Zamawiającego, po wcześniejszym ustaleniu operacyjnym z Zamawiającym sposobu postępowania w danej sytuacji. W sprawach technicznych usługa wsparcia świadczona będzie przez wykwalifikowany personel Wykonawcy, posiadający wiedzę i doświadczenie w zakresie świadczenia wsparcia, zgodnie z oficjalną polityką Producenta/ Producentów oferowanych rozwiązań. Niniejsza usługa wsparcia nie podlega procedurze odbioru.

**Instalacja i wdrożenie systemu bezpieczeństwa:**

1. Dostarczony system służący do zabezpieczenia infrastruktury komputerowej Zamawiającego powinien realizować wszystkie obecne funkcje sieciowe i bezpieczeństwa.
2. Realizowane prace wdrożeniowe nie mogą w żaden sposób zakłócić lub uniemożliwić prawidłowego funkcjonowania systemów informatycznych Zamawiającego. Prace „wrażliwe” - wymagające okna serwisowego muszą być wykonywane w obustronnie ustalonym terminie uzgodnionym pomiędzy Wykonawcą i Zamawiającym.
3. Wykonawca wykona połączenie dostarczonych urządzeń z siecią logiczną Zamawiającego.
4. Wykonawca zobowiązany jest do przeniesienia istniejących polityk (ok. 300 polityk), reguł dostępu i całej konfiguracji sieciowej z wykorzystywanego obecnie przez Zamawiającego systemu bezpieczeństwa do nowego systemu.
5. Wykonawca zintegruje dostarczone produkty zarówno pomiędzy sobą, jak i z elementami systemu teleinformatycznego Zamawiającego:
   1. system autoryzacji oparty o serwer LDAP,
   2. SIEM (syslog, definicja wszystkich pól)
   3. LibreNMS (monitoring parametrów pracy systemu).

**Formularz musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym (e-dowód).**

Pliki podpisywane profilem zaufanym, nie mogą być większe niż 10MB oraz pliki podpisywane w aplikacji eDoApp służącej do składania podpisu osobistego nie mogą być większe niż 5MB

***Zamawiający zaleca zapisanie formularza w formacie .pdf- z zastrzeżeniem, iż po zapisaniu muszą być widoczne wszystkie cytry i litery stanowiące treść Formularza przedmiotowo-cenowego***