Sękocin Stary, 15-07-2022 r.

Zn. spr.: DZ.270.90.2021

Wykonawcy

Dotyczy: postępowania o udzielenie zamówienia publicznego pn.: „**Zakup wielofunkcyjnych zapór sieciowych dla jednostek organizacyjnych Państwowego Gospodarstwa Leśnego Lasy Państwowe”**

Wyjaśnienia i zmiana treści SWZ

Zamawiający, działając na podstawie art.135 ust. 2 oraz art. 137 ust. 1 ustawy z dnia 11 września 2019 roku Prawo Zamówień Publicznych (t.j. Dz. U z 2021 r., poz. 1129 ze zm.)- zwanej dalej Pzp, w związku ze złożonymi wnioskami Wykonawców, przekazuje wyjaśnienia i zmianę treści SWZ;

Pytania I z dnia 04.07.2022 r.

Pytanie nr 2
SWZ Rozdział II pkt. 2 Czy Zamawiający dopuszcza aby karty katalogowe, potwierdzenia, że oferowane urządzenia dopuszczone do sprzedaży i użytkowania na terenie UE, zaświadczenie producenta urządzeń potwierdzające, że urządzenia posiadają certyfikat ICSA Labs lub EAL4 dla funkcji Firewall były w języku angielskim jeśli producent nie posiada wersji polskiej?
Odpowiedź:
Karty katalogowe, potwierdzenia oraz zaświadczenie producenta urządzeń potwierdzające, że urządzenia posiadają certyfikat ICSA Labs lub EAL4 dla funkcji Firewall lub Common Criteria Protection Profiles lub NSS Labs mogą zostać złożone w języku angielskim.

Pytanie nr 13
IPU Rozdział 3 § 18 Prosimy o podanie informacji jaki będzie okres gwarancji i serwisu w przypadku skorzystania z prawa opcji? Czy w przypadku Zamówienia opcji przed terminem wygaśnięcia Umowy czyli np. 41 miesiąca obowiązywania umowa w zakresie opcji będzie obowiązywać czy jednak kończy się po upływie 42 miesięcy?
Odpowiedź:
Uprawnienia gwarancyjne z tytułu prawa opcji będą nadal obowiązywać w zakresie gwarancji Producenta, przez okres wskazany w ofercie liczony od dnia dostawy urządzeń. Świadczenie usług serwisowych przez Wykonawcę będzie trwało od dnia dostarczenia urządzenia w ramach prawa opcji do końca terminu obowiązywania umowy.

Pytanie nr 14
IPU Rozdział 4 Termin wykonania umowy: Zgodnie z rozdziałem 4 Zamawiający podzielił termin realizacji umowy na klika etapów w terminie etap 0 na 8 dni roboczych od daty zwarcia umowy a Etap II na 50 dni Roboczych od zakończenia Etapu I. Jednakże mając na uwadze aktualne czasy dostaw urządzeń wyspecyfikowanych przez Zamawiającego, które to są sprzętem dedykowanym, termin wskazany przez Zamawiającego nie jest możliwy do dotrzymania przez żadnego wykonawcę, który nie posiada sprzętu na magazynie już na ten

moment. Zgodnie z informacją od producenta aktualne terminy dostawy urządzeń to 180 dni, gdyż są to produkty dedykowane pod to zamówienie i produkowane na bieżąco. Jednocześnie producent zastrzega sobie możliwość zmiany terminu w związku z panującą sytuacją COVID - 19, która ma wpływ na działanie łańcucha dostaw i dostępnością elementów do produkcji. Zatem zwracamy się z uprzejmą prośbą o wydłużenie dostawy urządzeń.

Odpowiedź:

§21 przyjmuje brzmienie

„Wykonawca zobowiązuje się do realizacji przedmiotu Umowy w następujących terminach:

1) *Etap 0 trwający 8 Dni Roboczych od dnia zawarcia Umowy, obejmuje: Testy wydajnościowe;*
2) *Etap I - trwający 21 Dni Robocze od dnia odbioru Etapu 0, obejmuje:*
   a) *Analizę przedwdrożeniową;*
   b) *Opracowanie Projektu Wdrożenia oraz Harmonogramu Szczegółowego;*
   c) *Opracowanie Planu oraz Scenariuszy Testów akceptacyjnych, na zasadach określonych w Załączniku nr 1 Do Umowy – OPZ.*
3) *Etap II – trwający do 115 Dni Roboczych od dnia odbioru Etapu I, obejmuje:*
   a) *Szkolenie autoryzowane dla Administratorów Technicznych z zakresu firewall UTM;*
   b) *Dostawę Systemu Centralnego Zarządzania i Logowania w CP wraz ze schematami konfiguracji oraz polityk bezpieczeństwa.*
   c) *Dostawę urządzeń do wszystkich jednostkach PGL LP zgodnie z Harmonogramem Szczegółowym.*
4) *Etap III – trwający do 50 Dni Roboczych od odbioru Etapu II, obejmuje:*
   a) *Wdrożenie konfiguracji oraz polityk bezpieczeństwa w jednostkach pilotażowych,*
   b) *Wdrożenie konfiguracji oraz polityk bezpieczeństwa w DGLP oraz pozostałych jednostkach PGL LP*
5) *Etap IV – trwający do 30 Dni Roboczych od dnia odbioru Etapu III, obejmuje:*
   a) *Wykonanie Dokumentacji;*
   b) *Szkolenie powdrożeniowe dla Administratorów Technicznych.*
6) *Etap V – trwający minimum 36 miesięcy od odbioru Etapu IV, obejmuje:*
   a) *Wsparcie serwisowe Wykonawcy;*
   b) *Wsparcie serwisowe Producenta wraz ze wszystkimi licencjami składającymi się na system firewall UTM."*

Pytanie nr 26

IPU Rozdział 12 § 85 Prosimy o podanie informacji jaki jest okres świadczenia Serwisu? Czy jest on równoznaczny z okresem gwarancji?

Odpowiedź:

Serwis producenta (zgodnie z ofertą wykonawcy) ma trwać przez okres równy okresowi gwarancji na dostarczone urządzenia. Serwis Wykonawcy ma trwać do końca obowiązywania umowy.

Zał.1 do SWZ w pkt.9 podp.2) lit. i przyjmuje brzmienie: „*Gwarancję producenta wraz z licencjami obejmującą wszystkie dostarczone Urządzenia wraz z oprogramowaniem, przy czym bieg okresu gwarancji oraz licencji w tym subskrypcji rozpocznie się z chwilą podpisania bez zastrzeżeń protokołu końcowego odbioru przedmiotu Umowy"*

Rozdział 12 §84 przyjmuje brzmienie: „*Wykonawca udziela Zamawiającemu minimum 36 miesięcznej gwarancji na dostarczoną Infrastrukturę, na zasadach określonych w Załączniku nr 1 do SWZ*"

Pytanie nr 43

Dotyczy paragraf 97 Umowy: Czy w przypadku awarii urządzenia UTM Zamawiający dopuści przy realizacji serwisu jego zwrot do producenta w przypadku, w którym to urządzenie nie jest wyposażone w dyski służące przechowywaniu logów mogących zawierać informacje wrażliwe a jedynie w nośniki danych służące przechowywaniu obrazu systemu operacyjnego i konfiguracji urządzenia? Takie podejście nie wymagałoby konieczności oferowania serwisu umożliwiającego w razie awarii pozostawienie całego urządzenia (w przypadku urządzeń bez wyjmowanych nośników danych), który stanowi dodatkowy, znaczący koszt całego rozwiązania.

Odpowiedź:

Zamawiający dopuszcza przy realizacji serwisu zwrot urządzeń do producenta w przypadku gdy urządzenia nie będą służyć do przechowywania „logów" mogących zawierać informacje wrażliwe.

Pytanie nr 44

Zamawiający wymaga dostarczenia w ramach dodatkowego kryterium do urządzenia z grupy II wkładek SFP kompatybilnych z Cisco. Prosimy o informację jaki rodzaj wkładek należy dostarczyć np.. Single-mode, multi-mode oraz czy to oznacza że należy dostarczyć 2szt wkładek: jedną kompatybilną z oferowanym urządzeniem a drugą z urządzeniami Cisco?

Odpowiedź:

Rozdział III ust.4 SWZ przyjmuje brzmienie:

4. Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1) Za ofertę najkorzystniejszą zostanie uznana oferta zawierająca najkorzystniejszy bilans punktów w kryteriach:

a) Łączna cena ofertowa brutto: (C) – 60% cena

Parametry techniczne (P_T) – 40% w tym:

*a) Kryterium **Czas usunięcia błędu** – waga **15%***

*b) Kryterium **Funkcjonalności dodatkowe system**u – waga **5%***

*c) Kryterium **okres licencji oraz gwarancji urządzeń** waga **20%***

2) Sposób obliczenia punktów:

*a) **Cena***

$$C = \frac{\text{Cena oferty z najniższą ceną (zamówienie podstawowe)}}{\text{Cena oferty badanej}} \times 60 \text{ (pkt)}$$

Ocena punktowa w kryterium „Łączna cena ofertowa brutto" dokonana zostanie na podstawie ceny ofertowej brutto wskazanej przez Wykonawcę w ofercie dla pozycji Cena ofertowa brutto za całość zamówienia podstawowego.

Liczba punktów przyznana poszczególnym ofertom zostanie obliczona z dokładnością do dwóch miejsc po przecinku albo z dokładnością wystarczającą do wykazania zróżnicowania ofert niepodlegających odrzuceniu.

*b) Kryterium **Czas usunięcia błędu krytycznego lub wysokiego** (C_{ub})– waga **15%***

*W kryterium „**Czas usunięcia błędu"** naprawa lub wymiana wadliwego podzespołu lub urządzenia ma zostać wykonana w 24 godzin od momentu przyjęcia zgłoszenia błędu. **W kryterium „Czas usunięcia błędu"** oferta może otrzymać maksymalnie 15 pkt.*

Zamawiający przyzna punkty, w zależności od deklaracji wykonawcy, za usunięcie błędu w okresie krótszym niż 24 godziny od momentu przyjęcia zgłoszenia błędu, w następujący sposób:

Usunięcie błędu w terminie 24 godzin od momentu przyjęcia zgłoszenia - Zamawiający przyzna - 0 pkt;
Usunięcie błędu w terminie 12 godzin od momentu przyjęcia zgłoszenia - Zamawiający przyzna - 10 pkt;
Usunięcie błędu w terminie 8 godzin od momentu przyjęcia zgłoszenia - Zamawiający przyzna - 15 pkt;

c) *Kryterium* ***Funkcjonalności dodatkowe system****u (F_d)– waga* ***5%***

W kryterium „Funkcjonalności dodatkowe systemu" *oferta może otrzymać maksymalnie 5 pkt. Za zadeklarowanie dostarczenia systemu spełniającego poniższe wymagania Zamawiający przyzna punkty w następujący sposób:*

Obsługa przez każde z oferowanych urządzeń firewall UTM wirtualnych domen w wysokości minimalnie trzech – 5 pkt.
W przypadku braku deklaracji Wykonawcy w formularzu ofertowym w tym zakresie Wykonawca otrzyma 0 punktów w tym kryterium.

d) *Kryterium* ***okres licencji oraz gwarancji urządzeń (O_{lg})*** *– waga* ***20%***

W kryterium „Licencjonowanie oraz system gwarancyjny" urządzenia oraz oprogramowanie muszą być objęte okresem wsparcia, serwisem gwarancyjnym producenta oraz okresem obowiązywania licencji wynoszącym 36 miesięcznym. W kryterium „Licencjonowanie oraz system gwarancyjny" oferta może otrzymać maksymalnie 20 pkt. Zamawiający przyzna punkty, w zależności od deklaracji wykonawcy, za dostarczenie licencji wraz ze wsparciem oraz serwisem gwarancyjnym producenta na okres:
Dostarczenie licencji wraz z usługą wsparcia oraz serwisem gwarancyjnym producenta na okres 36 miesięcy - 0 pkt;
Dostarczenie licencji wraz z usługą wsparcia oraz serwisem gwarancyjnym producenta na okres 48 miesięcy - 10 pkt;
Dostarczenie licencji wraz z usługą wsparcia oraz serwisem gwarancyjnym producenta na okres 60 miesięcy - 20 pkt;
Podanie okresu gwarancji krótszego niż 36 miesięcy będzie skutkowało odrzuceniem oferty jako niezgodnej z warunkami zamówienia.
Brak informacji w tym zakresie w tym zakresie będzie skutkował uznaniem przez Zamawiającego, że Wykonawca zaoferował licencje wraz z usługą wsparcia oraz serwisem gwarancyjnym producenta na okres 36 miesięcy.

3) *Za ofertę najkorzystniejszą uznana zostanie oferta, która uzyska łącznie najwyższą liczbę punktów obliczoną według wzoru:*

$$L = C + P_T$$

gdzie:

L – *całkowita liczba punktów,*

C – *punkty uzyskane w kryterium „Łączna cena ofertowa brutto",*

P_T – *punkty uzyskane w kryterium „Parametry techniczne",*

Ocena „Parametry techniczne" *dokonana zostanie na podstawie wskazanych w ofercie Wykonawcy parametrów technicznych zgodnie z punktacją określoną w SWZ dla kryterium „Parametry techniczne"*

4) *Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiadać będzie wszystkim wymaganiom przedstawionym w PZP oraz w SWZ i zostanie oceniona jako najkorzystniejsza w oparciu o podane kryteria wyboru.*
5) *Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że zostały złożone oferty o takiej samej cenie, Zamawiający wzywa wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych zawierających nową cenę.*

Zamawiający nie przewiduje przeprowadzenia dogrywki w formie aukcji elektronicznej"

Pytanie nr 45

Zamawiający wymaga dostarczenia w ramach wymagań podstawowych i wymagań dodatkowych do urządzenia z grupy III wkładek SFP/SFP+ kompatybilnych z Cisco. Prosimy o informację jaki rodzaj wkładek należy dostarczyć np.. Single-mode, multi-mode oraz czy to oznacza że należy dostarczyć 4szt wkładek SFP/SFP+: dwie kompatybilne z oferowanym urządzeniem oraz dwie kompatybilne z urządzeniami Cisco?

Odpowiedź:

Zamawiający dokonał zmiany kryteriów oceny ofert. Punkt 4.12 OPZ otrzymał brzmienie „Wkładki w ilości min. dwóch kompatybilnych z oferowanym urządzeniem oraz min. dwóch kompatybilnych z urządzeniami pracującymi w infrastrukturze zamawiającego dla urządzeń „CISCO" wkładki SFP+ winny być określone parametrami multi-mode; min. 10,0Gbps (SFP+); 2xLC (duplex); długość fali (TX/RX): 850nm; odległość transmisji do 300m; Układ Diagnostyki / Monitoring; Hot-Pluggable wraz z patchcordami światłowodowymi w ilości min. dwóch o długości min. 15m";

Pytanie nr 46

Zamawiający w kryterium funkcjonalności dodatkowe systemu wymaga trzech wirtualnych domen. Prosimy o potwierdzenie, że Zamawiający pisząc wirtualne domeny ma na myśli mechanizm wirtualizacji urządzenia umożliwiający separację ze względu na adresację, profile bezpieczeństwa, tablicę routingu, zarządzanie a nie jedynie wirtualizację ze względu na oddzielną tablicę routingu.

Odpowiedź:

Zamawiający określając „wirtualne domeny" miał namyśli mechanizm separacji wirtualnych urządzeń ze względu na profile bezpieczeństwa, tablicę routingu, adresację na jednym urządzeniu.

Pytanie nr 47

Zamawiający wymaga "Przygotowanie koncepcji wdrożenia łączy zapasowych z wykorzystaniem SD-WAN". Czy w związku z powyższym należy w ramach rozwiązania dostarczyć licencje SD-WAN?

Odpowiedź:

Zamawiający nie wymaga dostarczenia licencji dla rozwiązania SD-WAN, wymaga aby dostarczony system posiadał wsparcie technologii SD-WAN, umożliwiając w przyszłości rozbudowę systemu. Dlatego jednym z wymagań postawionych Wykonawcy przez Zamawiającego jest opracowanie koncepcji wykorzystania tej technologii w infrastrukturze PGL LP.

Pytanie nr 48

Zamawiający w ramach wdrożenia wyspecyfikował 11 jednostek pilotażowych. Czy to oznacza, że wykonawca powinien założyć, że ma wykonać instalację na miejscu w 11 jednostkach pilotażowych, a pozostałe w sposób zdalny korzystając z pomocy pracowników

Zamawiającego? (zakładamy wysłanie urządzenia skonfigurowanego, gdzie na miejscu pracownik Zamawiającego dokona przepięcia i wspólnie z wykonawcą wykona testy).
Odpowiedź:
Tak. Wykonawca powinien założyć, że ma wykonać instalację na miejscu w 11 jednostkach pilotażowych, a pozostałe w sposób zdalny korzystając z pomocy pracowników Zamawiającego.

Pytania II z dnia 04.07.2022 r.

Pytanie 1.
Dotyczy Załącznik 1 do SIWZ pkt 2.3)
Zamawiający wymaga, aby urządzenia typu Firewall UTM dla Nadleśnictw, Zakładów i Ośrodków posiadały obsługę minimum 37 tys. nowych sesji TCP na sek. Urządzenia Grupy I przeznaczone będą dla lokalizacji, w których znajdować się będzie średnio ok 30 osób, co oznaczałoby, że każdy z użytkowników musiałby generować ponad 1200 nowych sesji TCP/sek. W zestawieniu z pozostałymi wymaganymi parametrami wydajnościowymi wymóg ten wydaje się być mocno przeszacowany. Czy Zamawiający zgodzi się na dopuszczenie urządzeń obsługujących 32 tys. nowych sesji TCP na sek.? Pozwoli to na zaoferowanie optymalnego rozwiązania a jednocześnie zapewni odpowiedni zapas wydajności na poziomie ponad 1000 nowych sesji TCP/sek./użytkownika.
Odpowiedź:
Zamawiający pozostawia bez zmian zapisy Załącznik 1 do SIWZ pkt 2.3 dotyczące parametru określonego dla urządzeń Grupy I. Zamawiający określając przedmiotowy wymóg brał pod uwagę również możliwość rozbudowy systemu oraz możliwe zmiany organizacyjne w strukturze PGL LP.

Pytanie 2
Dotyczy Załącznik 1 do; SIWZ pkt 6.1 oraz pkt 8.15)
Zamawiający wymaga dostarczenia urządzeń wspierających architekturę SD-WAN.
Architektura SD-WAN oznacza zbiór wielu funkcjonalności a Zamawiający wymaga obsługi SD-WAN jedynie do przygotowania koncepcji wdrożenia dla łączy zapasowych, czyli małego wycinka funkcjonalności tej architektury. Czy w związku z powyższym dopuszczone zostanie rozwiązanie pozwalające na przygotowanie koncepcji wdrożenia łączy zapasowych w oparciu o zbudowanie na każdym z urządzeń kilku niezależnych tuneli VPN, w których ruch sterowany jest za pomocą dynamicznych protokołów routingu?
Odpowiedź:
Zamawiający wymaga aby dostarczony system posiadał wsparcie technologii SD-WAN, umożliwiając w przyszłości rozbudowę systemu. Dlatego jednym z wymagań postawionych Wykonawcy przez Zamawiającego jest opracowanie koncepcji wykorzystania tej technologii w infrastrukturze PG LP.

Pytanie 3
Dotyczy Załącznik 1 do SIWZ pkt 6.50)
Zamawiający wymaga: „Zarządzanie pasmem (QoS, Traffic shaping) za pomocą polityk powinny umożliwiać określenie adresów IP, portów, protokołów, aplikacji, użytkownika lub grupy użytkowników w oparciu o zewnętrznych dostawców tj. AD, zawierać pola DSCP.”
Czy Zamawiający dopuści rozwiązanie pozwalające na zarządzanie pasmem (Traffic shaping) za pomocą polityk powinny umożliwiać określenie adresów IP, portów, protokołów, aplikacji, użytkownika lub grupy użytkowników w oparciu o zewnętrznych dostawców tj. AD.?
Odpowiedź:

Zamawiający podtrzymuje określone wymagania. Dostarczony system musi umożliwiać ustawienie, zmianę wartości DSCP dla pakietów.

Pytanie 4

Dotyczy Załącznik 1 do SIWZ pkt 6.59.a)
Czy Zamawiający dopuści rozwiązanie, które realizuje dostęp do chronionych zasobów poprzez komunikację opartą o HTML 5.0 z wykorzystaniem zewnętrznego komponentu natywnie wspieranego przez oferowane rozwiązanie?
Odpowiedź:
Tak, jeżeli zewnętrzny komponent jest częścią oferowanego systemu i należy do producenta oferowanego systemu.

Pytania III z dnia 04.07.2022 r.

Pytanie 1

W dokumencie SWZ w p. III.4. Zamawiający określił kryteria dotyczące dodatkowej punktacji W kryterium oceny technicznej definiując wymaganie
“a) Kryterium Czas usunięcia błędu – waga 15%”.
Jednocześnie Zamawiający nie określił parametrów dotyczących błędu krytycznego. Może on bowiem odnosić się do awarii sprzętowej i konieczności wymiany uszkodzonych elementów co jest możliwe w krótkim okresie czasu. Należy jasno wskazać, iż w przypadku problemów związanych z oprogramowanie (potencjalny błąd/bug) to z naszej wiedzy wynika, że żaden z producentów nie jest w stanie usunąć takiego błędu i każdego błędu w czasie wymaganym przez Zamawiającego – tym samym nikt nie jest w stanie spełnić tego kryterium. Biorąc pod uwagę powyższe prosimy o uszczegółowienie jak Zamawiający określa „błąd krytyczny lub wysoki” i czy w szczególności dotyczy sytuacji, w której występuje konieczność wymiany urządzenia (RMA)? Ponadto prosimy o jednoznaczne wskazanie czy dla urządzeń pracujących w trybie wysokiej dostępności (HA, Typ 3), czas usunięcia błędu będzie liczony od uszkodzenie pojedynczego elementu czy też po uszkodzeniu urządzenia zapasowego
(drugiego, tzw. pasywnego)?
Odpowiedź:
Błąd krytyczny to błąd który uniemożliwia korzystanie z systemu: m.in. błędna konfiguracja, zła implementacja polityki bezpieczeństwa, uszkodzenie pojedynczego urządzenia niewynikające z niewłaściwego użytkowania. W przypadku błędów/bug-ów w oprogramowaniu producenta zamawiający wymaga wskazania sposobu rozwiązania problemu tzw. Workaround do momentu publikacji poprawki przez producenta.
W przypadku awarii urządzenia, niezależnie od grupy urządzeń, czas usunięcia błędu liczony jest od momentu uszkodzenia urządzenia

Pytanie 2

W dokumencie SWZ w p. III.4 Zamawiający określił kryteria dotyczące dodatkowej punktacji W kryterium oceny technicznej definiując wymaganie “b) Kryterium Funkcjonalności dodatkowe systemu – waga 5%” brzmiące “Obsługa przez każde z oferowanych urządzeń firewall UTM wirtualnych domen w wysokości minimalnie trzech – 5 pkt.”
Zamawiający definiując to wymaganie użył sformułowania właściwego dla jednego z producentów, zakładamy jednak, że celem Zamawiającego jest pozyskanie konkretnej funkcjonalności. Mając na uwadze różne architektury urządzeń Firewall UTM / NGFW istniejące na rynku oraz rożną nomenklaturę nazewnictwa prosimy o potwierdzenie, iż celem Zamawiającego jest by oferowane urządzenia zapewniały możliwość tworzenia niezależnych polityk bezpieczeństwa dla określonych segmentów sieciowych z możliwością przypisania do

nich wirtualnych routerów oraz definiowana wewnątrz urządzenia przepływów ruchu pomiędzy tymi wirtualnymi instancjami.

Odpowiedź:

Zamawiający zmienił kryteria oceny ofert - zgodnie z odpowiedzią na pyt. 44

Pytanie 3

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" w p.1.6. Zamawiający wymaga aby: Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje, które mogą zostać złożone w oryginale lub kopii poświadczającej zgodność z oryginałem: ICSA Labs lub EAL4 dla funkcji Firewall Prosimy o rozważenie zmiany lub wykreślenia całkowicie tego wymagania, ze względu na to, iż jego podtrzymanie może działać na szkodę Zamawiającego, ograniczać konkurencję i spowodować konieczność oferowania droższych i starszych urządzeń przez Wykonawców. Przedstawiamy poniżej kilka argumentów:

Jako Wykonawca przyjmujemy i rozumiemy, iż celem Zamawiającego jest zapewnienie, że otrzyma on w ofertach urządzenia sprawdzone oraz zweryfikowane pod kątem jakości sprzętowo programowej. Analizując jednak całościowo wymagania Zamawiającego opisane w dokumentach postępowania Zamawiający wprowadził szereg wymagań, zapewniających, iż urządzenia będą pochodziły od liderów rynkowych i uznanych producentów na świecie co jest wskazane w p.1.7. Załącznika nr 1 do SWZ „Opis przedmiotu zamówienia" wskazując, iż wymagania będzie mogło spełnić maksymalnie trzech producentów. Wszyscy Ci producenci mają wdrożone procedury zapewniające wysoką jakość sprzętu i oprogramowania oraz są stosowane w sieciach klientów strategicznych w krajach NATO.

Drugą istotną kwestią jest fakt, że na początku bieżącego roku czołowi producenci tego rozwiązań opisanych przez Zamawiającego tj. Checkpoint, Fortinet i Palo Alto ogłosiły dostępność nowych urządzeń firewall - które są z jednej strony tańsze, z drugiej wydajniejsze.

Jednocześnie biorąc pod uwagę proces certyfikacji urządzeń, który obecnie zajmuje do 2 lat wymaganie postawione przez Zamawiającego w p.1.7. powoduje, iż możliwe jest zaoferowanie urządzeń, które są dostępne na rynku od minimum 2-3 lat. Zamawiający pozbawia się tutaj z jednej strony dostępu do najnowszych technologii, potencjalnie godzi się na wyższą cenę, ale co też istotne pozyska platformy sprzętowe, które najprawdopodobniej w okresie obowiązywania 5-letniej umowy zostaną przez producentów wycofane ze sprzedaży, a co się z tym wiąże może dojść do sytuacji, w którym w czasie trwania umowy producent zaprzestanie rozwoju oprogramowania (będzie zapewnione tylko jego utrzymanie). Można też domniemywać, iż potencjalnie wszyscy dopuszczeni przez Zamawiającego producenci dążyć będą do certyfikacji nowych produktów w najszybszym możliwym czasie.

W kwestii samych certyfikacji chcemy również wskazać, że organizacja, która odpowiada za certyfikację EAL4 zaprzestała wykonywania walidacji EAL4 na poczet walidacji tzw. Protection Profiles (więcej informacji: https://www.niap-ccevs.org/Ref/FAQ.cfm#cat34) . Tym samym nie ma możliwości, aby w chwili obecnej nowe urządzenia uzyskały certyfikację EAL4, zaś urządzenia, które taką certyfikację posiadają są urządzeniami, których certyfikacja rozpoczęła się kilka lat temu. Alternatywą jest zmiana wymaganych historycznych certyfikatów do aktualnej i współczesnej formy - Common Criteria Protection Profiles – jednakże wprowadzenie tej certyfikacji (Network Devices Version min. wersja 2.1 oraz Stateful Traffic Filter Firewalls min. Wersja 1.3 dla urządzeń Firewall) spowoduje dalsze ograniczenie produktów, które Wykonawcy będą mogli zaoferować. Ostatnim czynnikiem, który chcielibyśmy podnieść to fakt, że Zamawiający wymaga certyfikacji dla samych urządzeń sieciowych i nie wymaga jej (lub równoważnej) dla systemów zarządzania, „podkładowych" systemów operacyjnych, itp. Tym samym występuje pewna niespójność wymagań dla całości systemu.

Podsumowując:
Wnosimy o wykreślenie wymagania 1.6 lub jego modyfikację w taki sposób by możliwe było zaoferowanie urządzeń, które pojawiły się na rynku w roku 2022. W przypadku zgody Zamawiającego Wykonawcy mieliby możliwość zaproponowania najnowszych rozwiązań liderujących producentów, których produkty w dłuższej perspektywie czasowej i tak poddawane są certyfikacji, W naszej ocenie odbyłoby się z korzyścią dla Zamawiającego, który uzyskałby z jednej strony dostęp na najnowszych generacji urządzeń, bardziej perspektywicznych w kwestii ich rozwoju w przyszłości, a z drugiej zyska niższą cenę zakupową.

Odpowiedź:

Pkt 1.6 Załącznik 1 do SIWZ przyjmuje brzmienie: „Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje, które mogą zostać złożone w oryginale lub kopii poświadczającej zgodność z oryginałem:

a) ICSA Labs lub EAL4 dla funkcji Firewall lub Common Criteria Protection Profiles lub NSS Labs;"

Rozdział II ust.5 pkt.3) SWZ przyjmuje brzmienie: „3)zaświadczenie producenta urządzeń potwierdzające, że urządzenia posiadają certyfikat ICSA Labs lub EAL4 dla funkcji Firewall lub Common Criteria Protection Profiles lub NSS Labs zgodnie z załącznikiem nr 1 OPZ pkt. 1.6"

Pytanie 4

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" w p.1.8. Zamawiający wymaga:
Wykonawca składając ofertę potwierdza, że dostarczone urządzenia spełniają wszystkie wymagania zawarte w OPZ. Wykonawca przedstawi kartę produktu zawierającą opis funkcjonalności i parametry, zamawiający dopuszcza wersję angielską Poszczególni producenci mają różną politykę dotyczącą umieszczania kluczowych danych w kartach katalogowych tym samym może się zdarzyć sytuacja, w której parametry, których potwierdzenia Zamawiający wymaga, nie będą się znajdować w karcie katalogowej.
W związku z powyższym prosimy o potwierdzenie, iż Zamawiający uzna ofertę za ważną, jeżeli Wykonawca przedstawi jako środki dowodowe dokumentację producenta w postaci odnośników do dokumentacji producenta umieszczonej na jego stronie internetowej lub też fragmentów dokumentacji w postaci załączników PDF, ewentualnie dopuszczenie oświadczeń i innych dokumentów potwierdzających spełnienie wymagań.

Odpowiedź:

Zamawiający dopuszcza złożenie oświadczenia własnego Wykonawcy potwierdzającego spełnienie wymagań dotyczących parametrów, które nie zostały wyszczególnione w karcie katalogowej.

Pytanie 5

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" w p.1.9. Zamawiający wymaga:
Dopuszcza się, by system centralnego zarządzania i logowania (Grupa IV), wchodzący w skład systemu ochrony był zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej dedykowanej platformy „virtual appliance".
Podobnie w punkcie 5 „Wymagania dla IV Grupy urządzeń centralnych do zarządzania i logowania w CP", Zamawiający zezwala na zastosowanie przez oferentów albo systemu zwirtualizowanego (VM Appliance) albo rozwiązania sprzętowego Uprzejmie prosimy o informację czy Zamawiający przewiduje dedykowanie określonych zasobów serwerowych (vCPU, RAM) i przestrzeni dyskowej dla potrzeb instalacji oprogramowania zarządzającego. Jeżeli tak to prosimy o wskazanie jaki są to zasoby. Prosimy też o wskazanie wirtualizatora (VMWare, Hyper-V, KVM), którym dysponuje Zamawiający celem doboru właściwej maszyny wirtualnej. Jeżeli zasoby te nie zostaną zapewnione przez Zamawiającego wówczas - biorąc

pod uwagę, iż system taki wymaga sprzętu - uprzejmie prosimy o potwierdzenie, że w przypadku dostarczenia systemu logowania i raportowania w postaci wirtualnej konieczne jest dostarczenie również wszystkich komponentów niezbędnych dla jego uruchomienia.
Alternatywnie prosimy o ujednolicenie wymagań przez określenie, iż system zarządzania musi zostać dostarczony w postaci dedykowanego urządzenia (appliance).

Odpowiedź:
Zamawiający określił wszelkie wymagane parametry oraz przedstawił środowisko jakim dysponuje, opis znajduje się w Załączniku nr 1 do SWZ pkt. 5.2.

Pytanie 6

W Załączniku nr 1 do SWZ w wymaganiach dla urządzeń Typ 1, Typ 2 oraz Typ 3 zamawiający używa opisu dla wydajności urządzenia "Przepustowość ruchu dla kontroli NGFW (Firewall, Application Control, IPS)" pomija jednak w tym wymaganiu malware (Punkt 46). Jednocześnie w innych wymaganiach funkcjonalnych Zamawiający określa wymagania inspekcyjne realizowane – praktycznie u wszystkich producentów - przez moduł antymalware.
Uprzejmie prosimy o wyjaśnienie czy nie doszło tutaj do oczywistej omyłki pisarskiej polegającej na nie uwzględnieniu w wymaganiu 46 funkcji antymalware. Pytanie z naszej strony jest o tyle istotne, że włączenie tej funkcjonalności może spowodować znaczącą (np. dwukrotną lub większą) degradację wydajności urządzenia w porównaniu do zestawu funkcji, który Zamawiający uwzględnił obecnie w wymaganiach. Jeżeli Zamawiający określił to wymaganie intencjonalnie wówczas prosimy w wskazanie dotyczące wymagań zamawiającego w kwestii wydajności urządzeń z włączonym silnikiem antymalware.
Dodatkowo prosimy o ewentualną/analogiczną zmianę w wymaganiach dotyczących testów wydajnościowych w p. 10.13.e.

Odpowiedź:
Punkty **2.6, 3.7, 4.7** Załącznika nr 1 do SWZ otrzymują brzmienie: „Przepustowość ruchu dla kontroli NGFW (Firewall, Application Control, IPS, antymalware) dla ruchu typu Enterprise*: minimum (…)" Przy zachowaniu podanych pierwotnie wartości odpowiednio dla każdej z grup.
Punkt 10.13.e Załącznika nr 1 do SWZ otrzymuje brzmienie:" Wydajność ruchu typu Enterprise nie mniej niż zgodnie z podaną specyfikacją w OPZ dla I,II grupy urządzeń kontroli NGFW (Firewall, Application Control., IPS, antymalware) Potwierdzeniem zaliczenia testu będzie raport z generatora ruchu zawierający informacje o przepływności ruchu. Zamawiający dopuszcza tolerancję błędu wynoszącą +/- 5%."

Pytanie 7

W Załączniku nr 1 do SWZ w wymaganiach dla urządzeń Typ 1, Typ 2 oraz Typ 3 Zamawiający wymaga dostarczenia urządzeń z podanymi ilościami interfejsów GigabitEthernet RJ-45 nie wymagając ilości dedykowanych interfejsów zarządzania.
Biorąc pod uwagę, że Zamawiający wymaga systemu zarządzania oraz wymaga lokalnego dostępu administracyjnego do urządzeń prosimy o wyjaśnienie czy należy przewidzieć, iż jeden z wymaganych portów jest przewidziany dla zarządzania czy też interfejs zarządzający ma być traktowany jako dodatkowy w urządzeniu danego typu (+1 do ilości podanej w wymaganiach)?

Odpowiedź:
Zamawiający nie wymaga dodatkowego portu zarządzania dla urządzeń Grupy I,II,III.

Pytanie 8

W Załączniku nr 1 do SWZ w wymaganiach dla urządzeń Typ 1, Typ 2 oraz Typ 3 Zamawiający wymaga obsługi VLAN z minimum 30 interfejsami.

W większości rozwiązań typu Firewall UTM / NGFW równocześnie do stosowania polityk bezpieczeństwa stosuje się pojęcie stref bezpieczeństwa (ang. zone). Prosimy o potwierdzenie iż właściwym jest rozumienie że wymaganie 30 interfejsów oznacza również wymaganie obsługi 30 stref (w połączeniu z wymaganiem z punktu 6.56.) ?

Odpowiedź:

Zamawiający określił wszelkie wymagane parametry minimalne stawiane dla urządzeń z grupy I,II,III w tym ilości interfejsów VLAN.

Pytanie 9

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" w p.4.4. Zamawiający wymaga aby:
W zakresie Firewall'a obsługa: minimum 160 tys. nowych sesji na sekundę TCP;
Z dokonanej analizy urządzeń dostępnych na rynku wynika, iż możliwe jest zaoferowanie urządzeń spełniających wymagania Zamawiającego z wyjątkiem tego jednego parametru. Analizowane urządzenie Palo Alto w zakresie firewalla obsługuje 155 tysięcy nowych sesji TCP na sekundę. Jednocześnie urządzenia te zapewniają wymagane wydajności na poziomie dwukrotnie wyższym niż wymagany. Spełnienie wymagania 4.4 w obecnej postaci spowoduje konieczność zaoferowania urządzeń, gdzie praktycznie wszystkie wymagane parametry będą przekroczone wielokrotnie, a tym samym cena tych urządzeń będzie adekwatnie wyższa (o około 100%).
Dodatkowo biorąc pod uwagę, że w opisie testów – w punkcie 10.13.f - Zamawiający dopuścił tolerancję testowanych wymagań w zakresie +-5% (czyli 8 tysięcy sesji na sekundę TCP) zmiana ta nie powinna stwarzać żadnych technicznych przeszkód, zwłaszcza że urządzenia te stosowane są sieciach klientów na całym świecie. W związku z powyższym prosimy o obniżenie wymagania 4.4 do poziomu 155 000 sesji TCP na sekundę.
Oczywiście mamy świadomość, że dobór parametrów technicznych (mimo, że spodziewamy się, iż został dokonany z pewnym zapasem) jest determinowany uzasadnionymi potrzebami Zamawiającego, jednakże w przypadku, gdy Zamawiający wyraziłby zgodę na obniżenie tego jednego parametru (realnie o mniej niż 4%) wówczas nam – jako Wykonawcy
– otworzy to możliwość złożenia oferty zdecydowanie korzystniejszej cenowo dla Zamawiającego.

Odpowiedź:

Zamawiający pozostawia bez zmian zapisy Załącznik 1 do SIWZ pkt 4.4 dotyczące parametru określonego dla urządzeń Grupy III. Istniejące zapisy są podyktowane uzasadnionymi potrzebami Zamawiającego.

Pytanie 10

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" w p.5.9 (a i b) . Zamawiający wymaga, aby centralny system zarządzania zapewniał:
a) minimum 500GB danych logów zdarzeń dziennie;
b) obsługę nie mniej niż 45TB przestrzeni dyskowej;
Prosimy o potwierdzenie czy przy realizacji systemu zarządzania i logowania składającego się z kilku aplikacji lub urządzeń wymagane jest spełnienie obu wymagań przez każdy z nich?

Odpowiedź:

Wymagania dotyczące systemu zarządzania oraz logowania zostały opisane w Załączniku nr 1 do SWZ w pkt. 5.8 oraz 5.9. W przypadku systemów rozdzielnych system zarządzania musi spełniać kryteria z pkt.5.8, a system logowania z pkt. 5.9. W przypadku systemów nierozdzielnych musi spełniać jednocześnie wymagania z pkt. 5.8 i 5.9.

Pytanie 11

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" w p.6.1.. Zamawiający wymaga aby

Urządzenia oferowane przez Wykonawcę muszą wspierać architekturę SD-WAN;
Prosimy o uszczegółowienie czy funkcjonalność (i ew. wymagane licencje) należy dostarczyć razem z urządzeniami, czy ma być tylko możliwość uzupełnienia licencji SD-WAN w przyszłości?
Odpowiedź:
Zamawiający nie wymaga dostarczenia licencji dla rozwiązania SD-WAN, wymaga aby dostarczony system posiadał wsparcie technologii SD-WAN, umożliwiając w przyszłości rozbudowę systemu. Dlatego jednym z wymagań postawionych Wykonawcy przez Zamawiającego jest opracowanie koncepcji wykorzystania tej technologii w infrastrukturze PGL LP.

Pytanie 12

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" w p.6.6.. Zamawiający wymaga aby cechą urządzeń była Współpraca z siecią energetyczną o parametrach: 230V AC ± 10%, 50 Hz +4% / – 6%;
Zamawiający definiuje wymaganie "Współpraca z siecią energetyczną o parametrach: 230V AC ± 10%, 50 Hz +4% / – 6%;"
Sposób, określenia wymagania w ten sposób powoduje, iż jego potwierdzenie jest trudne o ile wręcz niemożliwe w oficjalnej dokumentacji dominującej większości producentów. Biorąc pod uwagę, że kwestie zasilania są uregulowane normami i dyrektywami unijnymi wnosimy o potwierdzenie, że Zamawiający uzna to wymaganie za spełnione jeśli urządzenie będzie posiadało certyfikat zgodności CE jako wystarczające dla potwierdzenia zgodności z krajowym systemem energetycznym. Ewentualnie proponujemy o uzupełnienie wymagań (poza CE) o konieczność spełnienia dyrektyw unijnych 2014/30/EU oraz 2014/35/EU.
Podsumowując prosimy o zmianę tego zapisu do formy zgodnej z aktualnymi regulacjami prawnymi i normami EU.
Odpowiedź:
Pkt 6.6 Załącznik 1 do SIWZ przyjmuje brzmienie: „Współpraca z krajową siecią energetyczną o parametrach: 230/240V AC, 50/60 Hz".

Pytanie 13

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia".. Zamawiający wielokrotnie specyfikuje wymagania dotyczące technologii ochrony poczty elektronicznej przed spamem (SPAM):
- Punkt 6.19 "filtr WWW (...) spam (...)"
- Punkt 6.3 4 "(...)adresy e-mail(...)"
- Punkt 6.49 "Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3."
- Punkt 9.j "W ramach postępowania Wykonawca dostarczy licencje(...)Antyspam(...)"

Prosimy o rozważenie zmiany lub wykreślenia całkowicie tego wymagania, ze względu na to, iż jego podtrzymanie może działać na szkodę Zamawiającego i ograniczać konkurencję.
Przedstawiamy poniżej kilka argumentów:
Zamawiający w punkcie 1 "Wymagania ogólne" wymienia wymagane technologie bezpieczeństwa "Obejmuje kontrolą ochronę antywirusową, treści WWW, zaporę sieciową, system prewencji włamań (IPS), system detekcji zagrożeń (IDS), kontrolę aplikacji i usług." gdzie spam i ochrona poczty nie są wymienione.
Wymagania te są uzasadnione, gdyż dotyczą urządzeń stosowanych w sieci WAN. Znalazło to też odzwierciedlenie w zapisach przeprowadzanego przez Zamawiającego rozpoznania rynkowego (tzw. RFI) gdzie wymaganie na technologie Anty-SPAM oraz WAF nie byłby wymagane. Funkcjonalność Anty-SPAM jest właściwa dla urządzeń chroniących serwery pocztowe, w przypadku zatem gdy poczta elektroniczna jest realizowana za pomocą

scentralizowanego – całkowicie lub częściowo – rozwiązania, wówczas realizacja ochrony przed spamem również powinna być scentralizowana. Wielokrotnie zostało to potwierdzone w międzynarodowych rekomendacjach (np. NIST Special Publication 800-45 Version 2), iż efektywna realizacja ochrony przed spam powinna być realizowana w ramach systemu poczty elektronicznej i w punkcie przyjmowania poczty elektronicznej ze świata zewnętrznego
Z analizy rekordów typu MX w DNS dla domeny lasy.gov.pl, analizy historycznych Zamówień Publicznych Zamawiającego domniemujemy, że Zamawiający posiada już taki centralny system ochrony poczty elektronicznej. Replikowanie systemu anty-SPAM w kilkuset lokalizacjach (w których jak domniemujemy, nie ma już kilkuset lokalnych serwerów poczty elektronicznej) wymaga postawienia pytania o zasadność wymagania Anty-SPAM w urządzeniach stosowanych w WAN. Jednocześnie, utrzymanie wymagania dotyczącego funkcjonalności Anty-SPAM spowoduje ograniczenie producentów mogących zaoferować rozwiązania w przedmiotowym postępowaniu – w szczególności nie mogą tutaj zostać zaoferowane rozwiązania lidera rynku – firmy Palo Alto.
Podsumowując:
Wnosimy o wykreślenie wymagań dotyczących ochrony Anty-SPAM lub też modyfikację wymagań w taki sposób by możliwe było zaoferowanie urządzeń, które zapewniają pełną inspekcję protokołów poczty elektronicznej od strony sieciowej jednakże nie realizują ochrony anty-SPAM, która w ocenie Wykonawcy niekoniecznie jest niezbędna w miejscach gdzie wymaga jej Zamawiający.
Odpowiedź:
Zamawiający zmienia brzmienie Zał.1 do SWZ:
- pkt. 6.19 na następujące: „ramach filtra WWW powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, Dynamic DNS, proxy.”
- pkt 6.34 na następujący: ”Dostarczony system musi posiadać możliwość definiowania własnych list wskaźników IoC tj. sieci i adresy IP, nazwy DNS, skróty plików (co najmniej: SHA, MD5). Jeżeli jest to wymagane Wykonawca musi dostarczyć odpowiednie licencje producenta w ramach wskazanego rozwiązania;”
- pkt 9.j na następujący: „ramach postępowania Wykonawca dostarczy licencje równoważne z subskrypcją upoważniające do korzystania z aktualnych baz funkcji ochrony producenta obejmujące: kontrolę aplikacji, IPS, Antywirus, Web Filtering baz reputacji adresów IP/domen.”
Zamawiający wykreśla pkt 6.49

Pytanie 14

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia”.. Zamawiający w punkcie 6 określa “Wymagania wspólne dla I,II,III Grupy urządzeń tworzących system bezpieczeństwa. Wspólne dla wszystkich grup urządzeń.“ podpunkt 32 specyfikuje wymagania “Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.”, które w cyber-bezpieczeństwie określa się jako tzw. WAF (z ang. Web Application Firewall). Prosimy o rozważenie zmiany lub wykreślenia całkowicie tego wymagania, ze względu na to, iż jego podtrzymanie może działać na szkodę Zamawiającego i ograniczać konkurencję.
Mianowicie rozwiązania klasy WAF stosowane są w ośrodkach przetwarzania danych oraz w punktach styku z siecią Internet, w których udostępniane są aplikacje własne. W szczególności nie jest to cecha właściwa dla urządzeń w sieci WAN. Należy też zaznaczyć, iż chcąc w pełni zabezpieczyć lokalizacje zdalne w WAN przed atakami na aplikacje Web Zamawiający musiałby nabyć – zgodnie z rekomendacjami rynkowymi – dedykowane

rozwiązania, których funkcje znacząco wykraczają poza opisane w Załączniku 1 do SIWZ. Dedykowane rozwiązania są realizowane „zewnętrzne" względem zapór sieciowych i są dostarczane przez producentów takich jak A10, F5, Fortinet, Imperva, Radware czy podobnych przy czym wówczas koszt takiej ochrony byłby zapewne wyższy aniżeli koszt samych zapór.
Biorąc pod uwagę, iż funkcje opisane przez Zamawiającego stanowią najczęściej tylko uzupełnienie ochrony aplikacji prosimy o zmianę wymagania i dopuszczenie rozwiązań, które będą zapewniały inny podzbiór funkcjonalności WAF (w tym ochronę aplikacji webowych przed atakami typu: SQL injection, cross-site scripting (XSS), brute force, access violations, slowloris, security misconfigurations, Data Leak) przy czym jednak będzie to inny podzbiór względem wymaganego przez Zamawiającego.
Zmiana wymagania i dopuszczenie innej części funkcjonalnej WAF (w dużej mierze tożsamej z wymaganą) pozwoli Wykonawcy na zaoferowanie rozwiązań Palo Alto. Jednocześnie od strony technologicznej nie powinno wpływać to na jakość rozwiązania jako całości gdyż jako Wykonawca domniemujemy, iż podstawowa ochrona WAF jest realizowana dla aplikacji centralnych przez dedykowane rozwiązania.

Odpowiedź:
Zamawiający zmienia brzmienie Zał.1 do SWZ:
- pkt. 6.32 na następujące: „Mechanizmy ochrony dla aplikacji Web'owych co najmniej ochrona przed: Cross-site Scripting, SQL Injecton, Brute force."

Pytanie 15

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia".. Zamawiający w punkcie 6.34
Dostarczony system musi posiadać możliwość definiowania własnych list wskaźników IoC tj. sieci i adresy IP, nazwy DNS, adresy e-mail, skróty plików (co najmniej: SHA, MD5). Jeżeli jest to wymagane Wykonawca musi dostarczyć odpowiednie licencje producenta w ramach wskazanego rozwiązania; Powyższe wymaganie wskazuje zamkniętą listę IoC, których Zamawiający wymaga. Determinuje to pewien konkretny sposób realizacji usługi/funkcji. Ze względu na różne sposoby budowania sygnatur przez producentów rozwiązań Firewall UTM / NGFW nie zawsze jest możliwe blokowanie plików na bazie funkcji skrótów. Nie bez znaczenia jest to, iż funkcje skrótów są dziś bardzo wrażliwe na polimorfizm złośliwego oprogramowania przez co wartość bezpieczeństwa takiej funkcjonalności jest mocno ograniczona. Inną kwestią jest mocno ograniczona skalowalność takich list IoC; nota bene ograniczenie skalowalności dotyczy również adresów e-mail. Jednocześnie warto zaznaczyć, iż wiodący producenci oferują w swoich rozwiązaniach mechanizmy automatyzacyjne np. dla adresów IP, sieci IP czy domen. Część z nich oferuje również definiowania innych – również poddających się automatyzacji – wskaźników IoC, wykraczających poza listę wskazaną przez Zamawiającego.
W związku z powyższym prosimy o usunięcie z wymagania 6.34 fragmentu "adresy e-mail, skróty plików (co najmniej: SHA, MD5)."

Odpowiedź:
Zamawiający zmienia brzmienie Zał.1 do SWZ: pkt. 6.34 na następujące: „Dostarczony system musi posiadać możliwość definiowania własnych list wskaźników IoC tj. sieci i adresy IP, nazwy DNS, skróty plików (co najmniej: SHA, MD5). Jeżeli jest to wymagane Wykonawca musi dostarczyć odpowiednie licencje producenta w ramach wskazanego rozwiązania;"

Pytanie 16

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" Zamawiający w punkcie 6.35 określa wymaganie "System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików."

Funkcjonalność ta jest specyficzna dla wąskiej grupy (1-2) producentów rozwiązań typu NGFW/UTM i tym samym może ograniczać konkurencję. Biorąc pod uwagę aktualne uwarunkowania dotyczące sposobów ataków warto podkreślić, że złośliwe oprogramowanie dystrybuowane jest za pomocą małych i specjalnie spreparowanych dokumentów PDF/Office. Praktycznie nie spotyka się prawdziwych dokumentów firmowych wykorzystywanych w tym celu. Dodatkowo dopuszczenie dokumentów (bez aktywnej zawartości) i jednocześnie bez jego „manualnej" kontroli i analizy stanowić może poważne ryzyko naruszenia bezpieczeństwa w sieci Zamawiającego. Potencjalnym antidotum może być analiza Machine Learning realizowana bezpośrednio na urządzeniach, jednakże należy tu wskazać, iż w celu uzyskania pełnej pewności dotyczącej takiego pliku jest jego analiza w środowisku sandbox „baremetal" i dodatkowo ochrona realizowana samej stacji końcowej.
Czy w związku z tym prosimy o informację czy Zamawiający dopuści rozwiązanie, w którym pliki PDF oraz Microsoft Office będą poddawane kontroli i analizie przez moduły bezpieczeństwa (zgodnie z pozostałymi punktami w OPZ) wraz z analizą Machine Learning realizowaną na urządzeniu z możliwością ich zablokowania/zaraportowania w przypadku wykrycia zagrożenia, ale bez możliwości usunięcia aktywnej zawartości?
Odpowiedź:
Tak, Zamawiający dopuszcza wskazane w pytaniu rozwiązanie.
Zamawiający zmienia brzmienie pkt. 6.35 na następujące: „System musi umożliwiać kontrolę zawartości plików PDF oraz MS Office w przypadku wykrycia zagrożenia musi posiadać możliwość zablokowania oraz raportowania zagrożenia;"

Pytanie 17

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" Zamawiający w punkcie 6.38 określa wymaganie "System musi umożliwiać skanowanie archiwów, w tym co najmniej: ZIP, RAR."
Realizacja skanowania RAR przez urządzenia Firewall UTM jest możliwa tylko w trybie działania proxy, czyli działanie w archaicznym trybie Store and Forward. Wynika to z formatu archiwum RAR, które musi zostać pobrane w całości.
Jednocześnie dla pełnej analizy RAR i plików, które są skompresowane wewnątrz (zazwyczaj są to dokumenty Office) i tak konieczna jest ich analiza sandboxowa (statyczna lub dynamiczna) Stąd też prosimy o informację, czy Zamawiający dopuści możliwość realizacji skanowania RAR w chmurowym sandboxie tego samego producenta co oferowane zapory lub też prosimy o wykreślenie wymagania dotyczącego skanowania RAR.
Wykreślenie skanowanie zawartości RAR przez Firewall pozwoli Wykonawcom na zaoferowanie urządzeń Palo Alto Networks, które pracują w nowocześniejszym trybie inline ze strumieniową analizą treści. Jednocześnie sygnalizujemy, iż ze względu na techniczny sposób realizacji skanowania archiwów w urządzeniach działających w trybie proxy jest wysoce zalecane przeprowadzenie analizy wydajnościowej (dla tego trybu pracy zapór) lub
przyjęcie a priori, iż podane wartości w OPZ wydajności muszą uwzględniać przejście całego urządzenia w tryb proxy (z włączoną funkcją skanowania archiwów ZIP i RAR). Warto zaznaczyć, iż tryb proxy może być też wymuszany przez inne scenariusze ruchowe np. analizę DNS.
Przejście urządzenia w tryb proxy powoduje zazwyczaj ogromne ograniczenie jego wydajności (nieraz jest to. 10 krotny lub większy spadek). Oznacza to że w przypadku jeżeli Zamawiający rzetelnie określając potrzeby –wymagałby, aby wydajności urządzeń były realizowane w trybie proxy, wówczas koszty oferowanych urządzeń wzrosłyby kilkukrotnie.
Zmiana wymagania i dopuszczenie jako uzupełnienia innej części indykatorów IoC – dzięki automatyzacji znacznie częściej wykorzystywanych w praktyce - pozwoli Wykonawcy na

zaoferowanie rozwiązań Palo Alto. Jednocześnie od strony technologicznej nie powinno wpływać to na jakość rozwiązania jako całości, gdyż poza wymaganymi przez Zamawiającego urządzenia te oferują również możliwość definiowania innych wskaźników IoC.

Odpowiedź:

Zgodnie z wymogiem pkt. 6.38 System ma posiadać wskazaną funkcjonalność skanowania, Zamawiający nie narzuca sposobu realizacji wymogu.

Pytanie 18

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" Zamawiający w punkcie 6.53.b określa wymaganie:

System powinien zapewnić możliwość tworzenia polityk bezpieczeństwa z uwzględnieniem użytkowników;

- Użytkowników oraz grupy przechowywane w lokalnej bazie systemu,

- Użytkowników, grupy zagnieżdżone przechowywane w bazach zgodnych z LDAP,

- Atrybutów VSA zwracanych po uwierzytelnieniu użytkownika w serwerze RADIUS.

- Użytkowników oraz grupy przechowywane w bazach zgodnych z TACACS+;

W związku z coraz mniejszą popularnością uwierzytelnienia użytkowników z wykorzystaniem serwerów RADIUS oraz TACACS+ przy jednocześnie mocno rozwijanym uwierzytelnieniem z wykorzystaniem SAML prosimy o informacje czy Zamawiający zgodzi się na zaoferowanie zapór sieciowych, które umożliwią tworzenie polityk bezpieczeństwa z wykorzystaniem nazw użytkowników i grup przechowywanych w lokalnej bazie systemu, użytkowników i grup zagnieżdżonych przechowywanych w bazach zgodnych z LDAP oraz nazw użytkowników uzyskanych poprzez protokół SAML (jednocześnie zapory te nie obsługują atrybutów VSA zwracanych po uwierzytelnieniu w serwerze RADIUS oraz użytkowników i grup przechowywanych w bazach zgodnych z TACACS+). Ponadto oferowane zapory sieciowe zapewniałyby współpracę z rozwiązaniem Cisco ISE, którego rozbudowę Zamawiający przewiduje w ramach postępowania DZ.270.13.2022 Budowa Systemu Dostępu do Zasobów Sieciowych dla PGL LP.

Odpowiedź:

Zamawiający zmienia brzmienie Zał.1 do SWZ: pkt. 6.53b) na następujące: „

b) Użytkowników;

- Użytkowników oraz grupy przechowywane w lokalnej bazie systemu,
- Użytkowników, grupy zagnieżdżone przechowywane w bazach zgodnych z LDAP;"

Pytanie 19

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" Zamawiający w punkcie 6.59 określa wymaganie System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Prosimy o rozważenie zmiany tego wymagania jako opcjonalnego – dostępnego po rozbudowie. Rozwiązania SSL VPN stosowane są zazwyczaj na styku internetowym dla dostępu zdalnego użytkowników mobilnych lub pracowników działających w biurach zdalnych. Jako Wykonawca – mimo naszego wieloletniego doświadczenia – nie spotkaliśmy się z koniecznością realizowania dostępu zdalnego wewnątrz WAN w skali, której wymaga Zamawiający. Biorąc pod uwagę iż jest to element, który podnosi koszty rozwiązania (np.

koszty klienta VPN) prosimy o rozważenie wykreślenia tego wymagania lub jego ograniczenia dla części urządzeń w sieci, dla których opisana funkcja jest niezbędna lub całkowicie potraktowanie tego wymagania jako opcjonalnego (tzw. funkcje te będą dostępne po zakupie odpowiedniej licencji).

Odpowiedź:

Dostarczone urządzenia muszą posiadać możliwość realizacji funkcjonalności wskazanych w pkt 6.59. Zamawiający w przedmiotowym postępowaniu nie wymaga dostarczenia licencji.

Pytanie 20

W Załączniku nr 1 do SWZ „Opis przedmiotu zamówienia" Zamawiający w punkcie 6.59 określa wymaganie System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

W podpunkcie B Zamawiający wskazuje na konieczność zastosowania dedykowanego klienta. Uprzejmie prosimy o potwierdzenie, iż klienta tego należy dostarczyć wraz z urządzeniami, powinien pochodzić on od producenta oferowanych zapór i być objęty gwarancją i wsparciem technicznym producenta przez cały okres, na który jest wsparcie dla zapór sieciowych.

Odpowiedź:

Dostarczone urządzenia muszą posiadać możliwość realizacji wymagań wskazanych w pkt 6.59. Zamawiający nie wymaga w przedmiotowym postępowaniu dostarczenia licencji, gwarancji i wsparcia technicznego producenta dla dedykowanego klienta wskazanego w pkt. b.

Pytanie 21

W punkcie 10.7 OPZ opisane zostały wymagania odnośnie testów wydajnościowych:

"Testy muszą zostać wykonane dedykowanym urządzeniem dostarczonym przez Wykonawcę umożliwiającym wygenerowanie ruchu o wymaganej charakterystyce i wolumenie zgodnie ze specyfikacją minimalną przedstawioną w OPZ dla I,II grupy urządzeń firewall UTM. Urządzenie musi również umożliwiać generowanie próbek na podstawie pliku zawierającego podsłuchy lub skopiowany rzeczywisty ruch sieciowy."

Prosimy o uszczegółowienie charakterystyki ruchu, który będzie wykorzystywany na generatorze ruchu podczas testów wydajnościowych, przykładowo określając, że będzie to ruch zgodny z opisem z wymagań wydajnościowych w OPZ:

"ruch Enterprise (HTTPS - 32%; HTTP – 5%; LDAP – 25%; DNS – 1,6%; SMTP – 3,9%; UDP – 2,5%; TCP – 30%)" lub prosimy dołączyć próbkę ruchu (PCAP) która będzie mogła być wykorzystana podczas testów wydajnościowych do dokumentacji SWZ Zamówienia.

Pozwoli to Wykonawcy nie tylko na wcześniejsze przygotowanie się do testów, ale również zweryfikowanie oferowanych modeli przed złożeniem oferty Pragniemy podkreślić - Aby na etapie przygotowywania oferty możliwe było potwierdzenie spełnienia wymagań przez oferowane rozwiązania niezbędny jest dostęp do próbek ruchu PCAP, których zamierza użyć do testów Zamawiający. W przeciwnym wypadku nie ma możliwości weryfikacji wymagań w formie empirycznej a tylko za pomocą szacowania obarczonego bardzo dużym progiem błędów. Jeżeli dostarczenie próbek ruchu PCAP nie jest to możliwe, prosimy o wykreślenie wymagania z PCAP i pozostawienie tylko zapisu o ruchu "ruch Enterprise (HTTPS - 32%;

HTTP – 5%; LDAP – 25%; DNS – 1,6%; SMTP – 3,9%; UDP – 2,5%; TCP – 30%)" który zostanie wygenerowany za pomocą generatora ruchu / testera wydajności.

Odpowiedź:

Zamawiający podtrzymuje brzmienie przedmiotowych zapisów bez zmian – w ocenie Zamawiającego wszystkie wymagania zostały uwzględnione w zał. 1 do SWZ w sposób umożliwiający przygotowanie środowiska testowego.

Pytanie 22

Zamawiający zdefiniował dodatkową punktację oceny technicznej definiując wymaganie "d) Kryterium większe parametry niż minimalne wskazane w OPZ – waga 5%" przyznające dodatkowe punkty dla urządzeń wyposażonych w porty SFP dla Typ2 oraz SFP+ dla Typ3, odpowiednio 4pkt. oraz 1pkt.

Zamawiający przy takim wymaganiu wycenia na 4% wartości całej oferty (około 6,67% ceny całościowej przy budżecie ponad 19 mln zł daje 1,25 mln złotych) za dodatkowe dwa interfejsy sieciowe w 19 urządzeniach Typ 2. Wydaje się to być wartością astronomiczną. Ponieważ to wymaganie Zamawiającego jest opcjonalne, a z opisu wymagań wdrożeniowych nie wynika potrzeba realizacji dodatkowych połączeń światłowodowych wnosimy o jego wykreślenie albo zmniejszenie wagi punktowej za dodatkowe interfejsy SFP w urządzeniach Typ 2 na korzyść elementów, które wnoszą realną wartość dla Zamawiającego np. okres licencji i gwarancji.

Odpowiedź:

Zamawiający zmodyfikował kryteria oceny ofert - zgodnie z odpowiedzią udzieloną na pytanie nr 44.

Pytania IV z dnia 07.07.2022 r.

Pytanie 1.

Dotyczy Załącznik Nr. 1 do SIWZ Opis Przedmiotu Zamówienia. Wymagania Ogólne pkt 7.

Czy Zamawiający dopuści do udziału w postępowaniu producentów urządzeń Firewall UTM, którzy są uwzględnieni w kwadracie "Challengers" raportu Gartnera pt. „Magic Quadrant for Network Firewalls" na rok 2020 oraz 2021 pod warunkiem, iż tym samym okresie znaleźli się co najmniej raz w obszarze „Leaders" w innym raporcie, równoważnym do raportu Gartnera? Przykładem raportu równoważnego do Gartner Magic Quadrant for Network Firewalls jest np. raport The Forrester Wave: Enterprise Firewalls.

Odpowiedź:

Zamawiający nie wyraża zgody na proponowaną zmianę zapisu i podtrzymuje dotychczasowe zapisy.

Pytanie 2.

Dotyczy Załącznik Nr. 1 do SIWZ Opis Przedmiotu Zamówienia. wspólne dla I,II,III Grupy urządzeń tworzących system bezpieczeństwa. Wspólne dla wszystkich grup urządzeń pkt 1. Analiza OPZ prowadzi do wniosku, iż Zamawiający wymaga obsługi architektury SD-WAN jedynie do przygotowania koncepcji wdrożenia łączy zapasowych. Koncepcję tę można opracować w oparciu o inne, równoważne mechanizmy bez konieczności wykorzystywania architektury SD-WAN. W związku z powyższym czy Zamawiający dopuści jako równoważne rozwiązanie, które pozwala na stworzenie koncepcji łączy zapasowych w oparciu mechanizmy równoważne, np. dynamiczne tunele VPN?

Odpowiedź:

Zamawiający nie wymaga dostarczenia licencji dla rozwiązania SD-WAN, wymaga aby dostarczony system posiadał wsparcie technologii SD-WAN, umożliwiając w przyszłości rozbudowę systemu. Dlatego jednym z wymagań postawionych Wykonawcy przez

Zamawiającego jest opracowanie koncepcji wykorzystania tej technologii w infrastrukturze PGL LP.

Pytanie 3.
Dotyczy Załącznik Nr. 1 do SIWZ Opis Przedmiotu Zamówienia. Wymagania wspólne dla I,II,III Grupy urządzeń tworzących system bezpieczeństwa. Wspólne dla wszystkich grup urządzeń pkt. 40. W opisach wymagań dla poszczególnych grup urządzeń tylko dla grupy III należy zapewnić obsługę pracy w trybie HA. Prosimy o wyjaśnienie czy możliwość pracy w trybie HA Active/Active, Active/Passive wymagana jest dla urządzeń ze wszystkich grup, czy tylko urządzeń z grupy III?
Odpowiedź:
Funkcjonalność pracy w trybie HA wymagana jest dla wszystkich grup urządzeń. Uruchomienie pracy w trybie HA wymagane jest dla III grupy.

Udzielone odpowiedzi obowiązują Wykonawców przy składaniu ofert i będą stanowić załącznik do Załącznika nr 1 do umowy.
Stosownie do powyższego Zamawiający działając na podstawie art. 137 ust. 6 Pzp, w związku udzielonymi wyjaśnieniami oraz dokonanymi zmianami, zmienia następujące zapisy SWZ:

1) Zapisy Rozdziału III ust.2 pkt.1) przyjmują brzmienie:
„*Ofertę należy złożyć w terminie do dnia 09.08.2022 r. do godz. 09:00 za pośrednictwem formularza do złożenia oferty, zmiany oferty, wycofania oferty - dostępnego na ePUAP i udostępnionego również na miniPortalu. W formularzu oferty Wykonawca zobowiązany jest podać swój adres skrzynki ePUAP, za pośrednictwem której będzie prowadzona korespondencja z Wykonawcą związana z postępowaniem*."
2) Zapisy Rozdziału III ust.3 przyjmują brzmienie: „*Wykonawca pozostaje związany ofertą do dnia 06.11.2022 r. (tj. 90 dni od dnia składania ofert). Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.*"
3) Zapisy Rozdziału II ust.10 pkt.7) przyjmują brzmienie:
„Instrukcja wypełniania formularza JEDZ znajduje się na stronie internetowej Urzędu Zamówień Publicznych pod adresem:
https://www.uzp.gov.pl/__data/assets/pdf_file/0022/54904/Jednolity-Europejski-Dokument-Zamowienia-instrukcja-2022.04.29.pdf"
4) Załącznik nr 2 do SWZ (formularz oferty) przyjmuje brzmienie zgodne z załącznikiem do niniejszego dokumentu.
5) Załącznik nr 1 do SWZ (OPZ) przyjmuje brzmienie zgodne z załącznikiem do niniejszego dokumentu.
6) Załącznik nr 8 do SWZ – projekt umowy przyjmuje brzmienie zgodne z załącznikiem do niniejszego dokumentu.

Kierownik Zamawiającego:

Dariusz Gąsiorowski
Dyrektor Zakładu Informatyki
Lasów Państwowych