Warszawa, dn. 18.11.2020 r.

DYREKTOR GENERALNY
URZĘDU DO SPRAW CUDZOZIEMCÓW
Arkadiusz Szymański

BDG.WZP.261.18.2020/MW

dotyczy postępowania: **24/SYSTEM POBYT V.2-ROZBUDOWA MODUŁU OBSŁUGI SPRAW/PN/20**

Zamawiający informuje, że w związku z prowadzonym postępowaniem o udzielenie zamówienia publicznego na **zakup, dostawę i konfigurację urządzeń, licencji oraz zabezpieczeń typu firewall niezbędnych do zapewnienia poprawnego działania oraz zabezpieczenia Modułu Obsługi Spraw Systemu Pobyt v.2 na potrzeby Urzędu do Spraw Cudzoziemców**, w dniu 13 listopada 2020 r. wpłynęły pytania do treści Specyfikacji istotnych warunków zamówienia. W związku z powyższym, na podstawie art. 38 ust. 1 ustawy z dnia 29 stycznia 2004 roku - Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, z późn. zm.), zwanej dalej „ustawą Pzp", Zamawiający udziela wyjaśnień.

Pytanie 1:
Dotyczy opisu wymagań w p. 3 Załącznika nr 1b do SIWZ – Opis Przedmiotu Zamówienia.

W punkcie tym Zamawiający określił wymagania minimalne i parametry techniczne dla urządzeń UTM w taki sposób, iż najprawdopodobniej jedynym producentem mogącym je spełnić jest firma Juniper z wykorzystaniem urządzeń SRX1500 lub starszych modeli, jednakże przy założeniu, że dopuszczone zostanie chassis 2U lub zmieniona liczba modułów rozszerzeń.

Konstrukcja i zakres wymagań uniemożliwia złożenie ofert żadnemu z wiodących producentów, w tym żadnemu – poza Juniper - producentów notowanych z grupie liderów i tzw. challengers w raporcie MQ Gartnera z 2020 roku. Dotyczy to m.in. takich firm jak Checkpoint, Cisco, Fortinet, Huawei i Palo Alto Networks. Biorąc pod uwagę, iż pozostali producenci oferują uboższy zakres funkcji niż liderzy rynkowi to można poddać w wątpliwość czy któraś z pozostałych 11 firm notowanych jako znaczący producenci rozwiązań Firewall/UTM będzie mogła złożyć ofertę spełniającą wszystkie wymagania Zamawiającego.

W związku z powyższym mając na celu złożenie oferty na urządzeniach konkurencyjnych dla Juniper wnosimy o wprowadzenie zmian w OPZ. Szczegóły

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że wymaga spełnienia wymagań SIWZ oraz dopuszcza złożenie oferty na bazie produktów równoważnych do opisanych w Opisie Przedmiotu Zamówienia. Zamawiający przeprowadza postępowanie w sposób zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie Wykonawców, poprzez nie wskazywanie znaków towarowych, patentów lub pochodzenia produktów, czy też powoływania się na określonych producentów lub firmy, jedynie opisując przedmiot zamówienia w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty. Zgodnie z przywołanym wyrokiem Zespołu Arbitrów UZP z dnia 3 lutego 2005 UZP/ZO/0-153/05 „Zamawiający nie może dostosowywać SIWZ do warunków technicznych wygodnych dla poszczególnych Wykonawców, obniżając wymagania techniczne w odniesieniu do swoich potrzeb. Przyjęcie takiej tezy prowadziłoby do konieczności ciągłej zmiany wymagań i w konsekwencji dopuszczenia do postępowania Wykonawców, którzy nie oferują usług lub dostaw odpowiedniej (wcześniej zaplanowanej) jakości. Próba, bowiem ustalania wymagań technicznych zawartych, w SIWZ

przez Wykonawców a nie przez Zamawiającego prowadzi do zachwiania równowagi pomiędzy poszczególnymi Wykonawcami i w konsekwencji naruszenia przepisu art. 3 ustawy o zwalczaniu nieuczciwej konkurencji.”.

Odnosząc się do bezpodstawnego zarzutu jakoby Zamawiający preferował rozwiązania firmy Juniper, według najlepszej jego wiedzy istnieje przynajmniej kilka rozwiązań równoważnych renomowanych firm na rynku, które spełniają wymagania określone przez Zamawiającego w OPZ.

Pytanie 1 cd.
Grupa wymagań nr 1

- *Urządzenie dostarczane jest jako dedykowane urządzenie sieciowe 1 U, przystosowane do montażu w szafie rack.*
- *Urządzenie musi być wyposażone w co najmniej 4 GB pamięci RAM oraz dysk twardy SSD o pojemności nie mniej niż 100 GB. Do zarządzania out-of-band musi być przeznaczony dedykowany port Ethernet oraz port konsoli dostępny złączami RJ-45 oraz mini-USB.*
- *Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych.*
- *Urządzenie posiadać możliwość uruchomienia systemu operacyjnego z nośnika danych podłączonego do slotu USB w module kontrolnym*
- *Wraz z urządzeniem musi być dostarczony kabel RS-232 do podłączenia konsoli.*

Z racji tego, że urządzenia UTM stanowią zazwyczaj „zamkniętą” konstrukcję, gdzie producent określa pamięć minimalną niezbędną do działania urządzenia jak też jego interfejsy oraz zapewnia mechanizmy odzyskiwania oprogramowania systemowego wnosimy o zmianę tych wymagań na takie, które pozwolą Zamawiającemu na uzyskanie pożądanej funkcji urządzeń bez konieczności określenia sposobu realizacji przez producenta. Jednocześnie zmiana wymagania dopuszczającego urządzenia 2U pozwoli na dopuszczenie szerszego grona dostawców. Wnosimy o zmianę na

- *Urządzenie dostarczane jest jako dedykowane urządzenie sieciowe 2U, przystosowane do montażu w szafie rack*
- *Urządzenie musi być wyposażone w dysk twardy SSD o pojemności nie mniej niż 100 GB. Do zarządzania out-of-band musi być przeznaczony dedykowany port Ethernet oraz port konsoli.*
- *Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych*
- *Wraz z urządzeniem musi być dostarczony kabel do podłączenia konsoli.*

Odpowiedź Zamawiającego:
Zamawiający podtrzymuje wymagania i wyjaśnia, że w szafach serwerowych posiada bardzo mało miejsca, dlatego też Zamawiający oczekuje urządzenia o rozmiarze kompaktowym, które będzie wyposażone w zasoby sprzętowe pozwalające na wydajne i stabilne działanie w warunkach dużego obciążenia.

Pytanie 1 cd.
Grupa wymagań nr 2

- *Urządzenie musi być wyposażone w co najmniej 16 interfejsów Gigabit Ethernet 10/100/1000 TX, (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji) oraz nie mniej niż 4 interfejsów uplink 10 Gigabit Ethernet obsługujących wkładki SFP i SFP+. Wszystkie wbudowane interfejsy 1 Gigabit Ethernet muszą obsługiwać technologię PoE+ zgodnie z 802.3at.*
- *Urządzenie musi być wyposażone w nie mniej niż 4 sloty na dodatkowe karty z modułami interfejsów. Urządzenie musi umożliwić rozbudowę o co najmniej następujące rodzaje interfejsów: ADSL 2/2+, VDSL, 1 Gigabit Ethernet (SFP), 3G/LTE, wireless 802.11ac.*

Zestawienie wymagań dotyczących interfejsów uniemożliwia złożenie oferty przez żadnego z wiodących producentów. Wymagania dla portów PoE powodują, iż żaden z tych producentów nie jest w stanie zaproponować rozwiązań – o ile bowiem takie interfejsy są dostępne w relatywnie małych urządzeniach to nie spotyka się ich w rozwiązaniach oferujących 4 interfejsy 10GE lub więcej. Podobnie rzecz się ma w przypadku modułów do rozbudowy – w dominującej większości producenci oferują możliwości rozbudowy o dodatkowe interfejsy Ethernet (Cisco, Checkpoint) lub preferują urządzenia o zamkniętym, lecz zwykle rozbudowanym spektrum interfejsów (Fortinet, Huawei, Palo Alto). Biorąc to pod uwagę prosimy o całkowite usunięcie wymagania dotyczącego modułów rozbudowy ADSL, VDSL, 3G, wireless. W przypadku interfejsów Ethernet wnosimy o urealnienie potrzeb zamawiającego w odniesieniu do liczby interfejsów oraz o zmianę wskazującą bądź minimalną liczbę interfejsów i wymagane możliwości rozbudowy lub wskazanie docelowej liczby interfejsów wymaganych przez Zamawiającego.

- *Urządzenie musi być wyposażone w co najmniej*

1. *4 interfejsów uplink 10 Gigabit Ethernet obsługujących wkładki SFP i SFP+ LUB alternatywnie 4 interfejsów 10 Gigabit Ethernet SFP+ i 4 interfejsów 1 Gigabit Ethernet SFP*
2. *4 interfejsów Gigabit Ethernet 10/100/1000 TX*
3. *4 interfejsów Gigabit Ethernet SFP*

Odpowiedź Zamawiającego:
Zamawiający podtrzymuje wymagania i wyjaśnia, że oczekuje podanej gęstości portów oraz elastyczności w doborze rodzajów interfejsów sieciowych. Zamawiający nie wymaga rozbudowy o dodatkowe porty 1GbE, biorąc pod uwagę podstawowe wymaganie 16 portów 10/100/1000 oraz 4 porty uplink. Zamawiający podtrzymuje wymaganie dotyczące portów PoE+.

Pytanie 1 cd.
Grupa wymagań nr 3

- *Urządzenie musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 120 strefami bezpieczeństwa z wydajnością nie mniejszą niż 4 000 Mb/s liczoną dla ruchu IMIX. Firewall musi przetworzyć nie mniej niż 1 700 000 pakietów/sekundę (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż 375 000 równoległych sesji oraz zestawić nie mniej niż 48 000 nowych połączeń/sekundę. Firewall musi realizować funkcje zabezpieczeń w trybie warstwy 3 i warstwy 2 modelu OSI.*

Zamawiający określa wymagania dla firewalla L3 – które obecnie praktycznie nie znajdują zastosowania gdyż w większości implementacji dostępnych na rynku w postaci urządzeń UTM/NGFW wykorzystywana jest funkcjonalność rozpoznawania aplikacji, która jest bardziej wymagająca jeżeli chodzi o zasoby. Tym samym realne parametry wydajnościowe urządzenia UTM są określone przez dane dotyczące firewalla aplikacyjnego.

Jednocześnie Zamawiający w innym punkcie wymagań określa, iż urządzenie powinno posiadać wydajność dla ruchu z rozpoznawaniem aplikacji na poziomie 1000 Mb/s, co stoi w sprzeczności z wymaganiami określonymi powyżej. Ponadto wskazane wymagania określają specyficzne urządzenia/produkt. Wnosimy o wykreślenie tego wymagania oraz wskazanie realnych oczekiwań Zamawiającego w kontekście firewalla aplikacyjnego i odniesienia wymagań do parametrów aplikacyjnych np. http 64K aniżeli typowo sieciowych (np. IMIX).

- *Urządzenie musi realizować zadania Stateful Firewall oraz firewalla aplikacyjnego z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji z wydajnością nie mniejszą niż 2 000 Mb/s.*
- *Urządzenie musi obsłużyć nie mniej niż 40 stref bezpieczeństwa*

- *Firewall musi obsłużyć nie mniej niż 180 000 równoległych sesji oraz zestawić nie mniej niż 12 000 nowych połączeń/sekundę.*
- *Firewall musi realizować funkcje zabezpieczeń w trybie warstwy 3 i warstwy 2 modelu OSI.*

Odpowiedź Zamawiającego:
Zamawiający podtrzymuje wymagania i wyjaśnia, że dla części ruchu nie przewiduje zastosowania mechanizmów UTM/NGFW oraz rozpoznawania aplikacji, stąd urządzenie musi spełniać również określone parametry wydajności dla funkcji „tradycyjnego" stateful firewalla.

Pytanie 1 cd.
Grupa wymagań nr 4

- *Urządzenie musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE v2 w konfiguracji site-to-site oraz client-to-site. Firewall musi obsługiwać nie mniej niż 2 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 1 Gb/s dla ruchu IMIX. W zakresie VPN urządzenie musi obsługiwać zestawianie tuneli VPN w oparciu o certyfikaty oraz standardowe algorytmy kryptograficzne, w tym AES256, SHA-256, DH14. W celu obsługi architektury VPN hub&spoke firewall musi obsługiwać funkcje Auto VPN i Auto Discovery VPN. Urządzenie musi posiadać możliwość zestawienia tuneli VPN z użytkownikami łączącymi się przy pomocy oprogramowania klienta VPN w oparciu o protokoły IPSec VPN i SSL VPN.*
- *Urządzenie musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE v2 w konfiguracji site-to-site oraz client-to-site. Firewall musi obsługiwać nie mniej niż 2 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 1 Gb/s dla ruchu IMIX. W zakresie VPN urządzenie musi obsługiwać zestawianie tuneli VPN w oparciu o certyfikaty oraz standardowe algorytmy kryptograficzne, w tym AES256, SHA-256, DH14. W celu obsługi architektury VPN hub&spoke firewall musi obsługiwać funkcje Auto VPN i Auto Discovery VPN. Urządzenie musi posiadać możliwość zestawienia tuneli VPN z użytkownikami łączącymi się przy pomocy oprogramowania klienta VPN w oparciu o protokoły IPSec VPN i SSL VPN.*

Zamawiający wymaga w tym punkcie funkcjonalności VPN, która w większości jest realizowana przez większość dostawców, jednocześnie wskazuje jednak na funkcje własnościowe producenta w postaci Auto VPN i Auto Discovery VPN. Wnosimy o ich wykreślenie oraz o zmianę wymagania na

- *Urządzenie musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE (v1 lub v2) w konfiguracji site-to-site oraz client-to-site. Firewall musi obsługiwać nie mniej niż 2 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 1 Gb/s. W zakresie VPN urządzenie musi obsługiwać zestawianie tuneli VPN w oparciu o certyfikaty oraz standardowe algorytmy kryptograficzne, w tym AES256, SHA-256, DH14. Urządzenie musi posiadać możliwość zestawienia tuneli VPN z użytkownikami łączącymi się przy pomocy oprogramowania klienta VPN w oparciu o protokoły IPSec VPN i SSL VPN.*

Odpowiedź Zamawiającego:
Zamawiający podtrzymuje wymagania i wyjaśnia, że Auto VPN i Auto Discovery VPN nie są funkcjami własnościowymi konkretnego producenta, ale standardami opisanymi np. w IETF - RFC 7018., które odnoszą się do architektury połączeń IPSec VPN site-to-site, a nie połączenia z programowego klienta VPN.

Pytanie 1 cd.
Grupa wymagań nr 5

- *Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 4 000 reguł polityki bezpieczeństwa.*

- *Urządzenie musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z aplikacjami typu Peer-to-Peer i Instant Messaging). Identyfikacja aplikacji musi odbywać się co najmniej przez sygnatury i analizę heurystyczną. Urządzenia musi identyfikować nie mniej niż 3500 różnych aplikacji, w szczególności takich, które są tunelowane w protokołach HTTP i HTTPS – w tym aplikacji Web 2.0, nie mniej niż Skype, Facebook, Youtube. Musi być dostępna możliwość definiowania własnych sygnatur aplikacji z uwzględnieniem kryteriów z warstwy 7 modelu OSI. Dostęp użytkowników do poszczególnych aplikacji musi być konfigurowany przy pomocy reguł filtrowania uwzględniających co najmniej adresy IP, nazwy użytkowników oraz wyżej wymienione aplikacje. Kontrola dostępu do dynamicznie identyfikowanych aplikacji musi być wykonywana z przepustowością nie mniej niż 1 000 Mb/s mierzoną dla transakcji HTTP o długościach 44 KB.*

Wymagania określone w tym punkcie ponownie odnoszą się do konkretnych parametrów urządzenia Juniper. Wnosimy o zmianę wymagań mającą na celu zwiększenie konkurencyjności – przede wszystkim w postaci wykreślenia rodzaju transakcji http o długości 44KB gdyż parametr ten stosowany jest tylko przez firmę Juniper i firmę Forcepoint (której urządzenia nie spełniają wymagań OPZ) – tym samym ogranicza to konkurencję. Wnosimy też o zmniejszenie liczby obsługiwanych reguł polityki bezpieczeństwa do 1500, która to wartość jest bardziej adekwatna względem pozostałych wymagań Zamawiającego. Jednocześnie wnosimy o uspójnienie wymagań dotyczących przepustowości firewalla dla kontroli dostępu do dynamicznie identyfikowanych aplikacji (wspomniane też w pytaniu w Grupie wymagań nr 3). Wnosimy o zmianę wymagania na:

- *Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 1 500 reguł polityki bezpieczeństwa.*

- *Urządzenie musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z aplikacjami typu Peer-to-Peer i Instant Messaging). Identyfikacja aplikacji musi odbywać się co najmniej przez sygnatury i analizę heurystyczną. Urządzenia musi identyfikować nie mniej niż 3500 różnych aplikacji, w szczególności takich, które są tunelowane w protokołach HTTP i HTTPS – w tym aplikacji Web 2.0, nie mniej niż Skype, Facebook, Youtube. Musi być dostępna możliwość definiowania własnych sygnatur aplikacji z uwzględnieniem kryteriów z warstwy 7 modelu OSI. Dostęp użytkowników do poszczególnych aplikacji musi być konfigurowany przy pomocy reguł filtrowania uwzględniających co najmniej adresy IP, nazwy użytkowników oraz wyżej wymienione aplikacje. Kontrola dostępu do dynamicznie identyfikowanych aplikacji musi być wykonywana z przepustowością nie mniej niż 2 000 Mb/s.*

Odpowiedź Zamawiającego:
Zamawiający podtrzymuje wymagania. Podana przepustowość i długość transakcji HTTP mają znaczenie referencyjne. Zamawiający oczekuje urządzenia o parametrach wydajnościowych nie gorszych, niż podane, a nie dokładnie takich. Podanie referencyjnej wartości ma na celu wykluczenie ofert, w których wydajności określone są dla nierealistycznych warunków pomiarów. Nie istnieje zdefiniowany standard metodologii pomiarów dla urządzeń klasy Firewall/NGFW/UTM. Dobór takiej, a nie innej wartości długości transakcji jest arbitralnym wyborem Zamawiającego opartym na uwarunkowaniach w swojej sieci, obserwowanego profilu ruchu, itp.

Pytanie 1 cd.
Grupa wymagań nr 6

- *Urządzenie musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention). System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych rodzajów ataków musi odbywać się w regułach polityki bezpieczeństwa. System firewall musi realizować zadania IPS z wydajnością nie mniejszą niż 2 000 Mb/s mierzoną dla transakcji HTTP o długościach 44 KB. Baza sygnatur*

IPS musi być utrzymywana i udostępniana przez producenta urządzenia, nie może zawierać mniej niż 10 000 pozycji. Baza sygnatur ataków musi być aktualizowana codziennie. Musi być dostępna możliwość definiowania własnych sygnatur ataków.

- *Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antywirusowej sprawdzający komunikację związaną z pocztą elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać instalowania dodatkowego serwera przez użytkownika. W celu optymalizacji działania, baza definicji wirusów i złośliwego oprogramowania nie powinna być ściągana lokalnie na urządzenie – porównywanie charakterystyki badanego ruchu z wzorcami wirusów powinno odbywać się w serwisie udostępnionym przez producenta.*

Zamawiający w powyższych wymaganiach określa wymagania dla blokowania intruzów i ochrony antywirusowej. Zamawiający wskazuje przy tym bardzo konkretny sposób realizacji tego wymagania, który praktycznie uniemożliwia konkurencję. Pierwszym z kryteriów jest określenie wymagań wydajnościowych pod kątem transakcji http 44KB, które jest powtarzane w wielu wymaganiach, Zamawiający określa też wymaganie wydajności IPS na poziomie 2Gbps jednocześnie wymagając, aby silnik IPS był uruchomiony w polityce bezpieczeństwa, a w innym punkcie specyfikacji wymaganie dla firewalla aplikacyjnego, który ma być częścią polityki jest określone na poziomie 1Gbps. Wnosimy w związku z tym o zmianę wymagania dla silnika IPS na 1Gbps.

Wnosimy także o wykreślenie wymagania wskazującego, iż baza sygnatur IPS nie może zawierać mniej niż 10 000 pozycji. Jest to wymaganie, które jest mocno powiązane ze sposobem liczenia sygnatur przez producentów – część z nich pojedynczą sygnaturę uznaje tylko dla głównego ataku, a poszczególne jego mutacje są ukryte pod jednym wpisem. Inni producenci każdą z mutacji opisują pod osobną sygnaturą. Oznacza to iż nie ma prostego mechanizmu pozwalającego na określenie, iż baza producenta z pierwszej grupy jest gorsza od tego z grupy drugiej – może się bowiem okazać, iż baza z potencjalnie mniejszą nominalną liczbą sygnatur jest bogatsza i pozwala na uzyskanie lepszej ochrony.

W kwestii aktualizacji bazy IPS, w odróżnieniu od bazy antywirusowej jest ona w przypadku implementacji większości producentów bardziej „statyczna" i nie jest aktualizowana codziennie o ile nie ma takiej konieczności. Z drugiej strony w przypadku zaistnienia zagrożeń bazy te mogą być aktualizowane częściej niż raz dziennie. W związku z powyższym wnosimy o wykreślenie tego wymagania, co wpłynie na zwiększenie konkurencyjności.

W punkcie dotyczącym ochrony antywirusowej Zamawiający wskazuje konkretny model realizacji wymaganej funkcjonalności co powoduje znaczące ograniczenie konkurencji. Wnosimy o wykreślenie zapisów, które nie określają oczekiwanej funkcjonalności a jedynie konkretny sposób realizacji – w naszej ocenie nie uzasadniony w tym przypadku. Wnosimy zatem o zmianę tych wymagań na następujące brzmienie

- *Urządzenie musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention). System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych rodzajów ataków musi odbywać się w regułach polityki bezpieczeństwa. System firewall musi realizować zadania IPS z wydajnością nie mniejszą niż 1 000 Mb/s. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia. Musi być dostępna możliwość definiowania własnych sygnatur ataków.*

- *Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antywirusowej sprawdzający komunikację związaną z pocztą elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać instalowania dodatkowego serwera przez użytkownika.*

Odpowiedź Zamawiającego:
Zamawiający podtrzymuje wymagania dotyczące funkcji wykrywania i blokowania ataków intruzów (IPS, intrusion prevention). Zamawiający wyjaśnia, że zdefiniowanie progu rozmiaru bazy IPS jest

ul. Taborowa 33
02-699 Warszawa
tel. 22 601 74 01-03
fax 22 601 74 13
kierownictwo@udsc.gov.pl
www.udsc.gov.pl

kluczowe do rozróżnienia między rozwiązaniami IPS i rozwiązaniami, które nimi nie są, opierając się na np. jedynie na kilku statycznych wzorcach ataku, anomalii.
W związku z powyższym **Zamawiający** na podstawie art. 38 ust. 4 ustawy Pzp, **dokonuje zmiany zapisu** w załączniku nr 1b do SIWZ, gdzie zapis o następującym brzmieniu:

„Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antywirusowej sprawdzający komunikację związaną z pocztą elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać instalowania dodatkowego serwera przez użytkownika. W celu optymalizacji działania, baza definicji wirusów i złośliwego oprogramowania nie powinna być ściągana lokalnie na urządzenie – porównywanie charakterystyki badanego ruchu z wzorcami wirusów powinno odbywać się w serwisie udostępnionym przez producenta."

otrzymuje następujące brzmienie:
„Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antywirusowej sprawdzający komunikację związaną z pocztą elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać instalowania dodatkowego serwera przez użytkownika.".

Pytanie 1 cd.
Grupa wymagań nr 7

- *Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF, IS-IS oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 128 wirtualnych routerów. Firewall musi obsługiwać następujące protokoły routingu dynamicznego IPv6: RIPng, OSPFv3, BGP. Pojemność tablicy routingu musi wynosić nie mniej niż 1 milion tras.*
- *Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN.*

Zamawiający określa w powyższych wymagania funkcje dotyczące routingu. Zakres wymaganych protokołów oraz pojemność tablic routingu znacząco odbiega od zakresu realizowanego przez urządzenia wiodących producentów i ogranicza konkurencję do rozwiązań posiadających bardzo niszowe funkcje – najprawdopodobniej nie wykorzystywane w sieci wewnętrznej Zamawiającego. Celem dostosowania wymagań do realnych potrzeb oraz zwiększenia konkurencyjności wnosimy o jego zmianę na:

- *Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 5 wirtualnych routerów. Firewall musi obsługiwać następujące protokoły routingu dynamicznego IPv6: OSPFv3, BGP.*

Odpowiedź Zamawiającego:
Zamawiający podtrzymuje wymagania i zastrzega sobie prawo do dowolnego korzystania z pełni funkcji oferowanych na uniwersalnych urządzeń bezpieczeństwa dostępnych na rynku – również w zakresie routingu.

Pytanie 1 cd.
Grupa wymagań nr 8

- *Urządzenie musi obsługiwać co najmniej 3000 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły Spanning Tree (802.1D), Rapid STP (802.1w) oraz Multiple STP (802.1s). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet. Pojemność tablicy adresów MAC nie może być mniejsza niż 16 000.*
- *W celu zapewnienia bezpieczeństwa danych przesyłanych w warstwie 2 urządzenie musi obsługiwać protokół MACSec zgodnie z 802.1AE na wszystkich wbudowanych portach 1 Gigabit Ethernet i 10 Gigabit Ethernet. Dane przesyłane protokołem MACSec muszą być zabezpieczone algorytmem szyfrowania AES z kluczem o długości nie mniej niż 256 bitów.*

- *Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach.*

Zamawiający określa w powyższych wymagania funkcje dotyczące warstwy sieciowej. Są one jednak bardziej właściwe dla rozwiązań klasy router lub przełącznik warstwy trzeciej. Bardzo rozbudowane wymagania w tym zakresie powodują, iż większość producentów nie może spełnić oczekiwań Zamawiającego. Wymagania dotyczące obsługi 802.1AE w powiązaniu z wymaganiami dla grupy protokołów Spanning Tree oraz dla mechanizmu WRED spełnia najprawdopodobniej tylko jeden dostawca. Wnosimy zatem o zmianę wymagań i dostosowanie ich do realnych potrzeb, co spowoduje zwiększenie konkurencyjności. Wnosimy o zmianę tych wymagań na:

- *Urządzenie musi obsługiwać co najmniej 3000 sieci VLAN z tagowaniem 802.1Q (obsługa 4094 znaczników).*
- *Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach*

Odpowiedź Zamawiającego:
Zamawiający podtrzymuje wymagania. Jest to podstawowy zakres wymagań na funkcje L2 oferowany przez większość producentów urządzeń zabezpieczeń. Według najlepszej wiedzy Zamawiającego istnieje przynajmniej kilka rozwiązań równoważnych renomowanych firm na rynku, które spełniają wymagania.

Pytanie 2:
Dotyczy opisu wymagań w p. 3 Załącznika nr 1b do SIWZ – Opis Przedmiotu Zamówienia.

Zamawiający określa wymagania funkcje dotyczące filtrowania zawartości ruchu.

- *Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies*

Wymaganie to jest jednak określone nieprecyzyjnie, gdyż można je rozumieć jako konieczność filtrowania ruchu na podstawie wszystkich podanych kryteriów we wszystkich podanych protokołach. Wykonawca pragnie zauważyć, iż tzw. cookies występują tylko w komunikacji HTTP co oznacza, iż wymaganie ich blokowania dla poczty elektronicznej nie ma zastosowania. Prosimy o potwierdzenie, że Zamawiający oczekuje filtracji ruchu na podstawie wskazanych kryteriów zależnie od typu ruchu i uzna ofertę za ważną, jeżeli urządzenie nie będzie umożliwiało np. blokowania cookies w ruchu FTP.

Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że oczekuje filtracji zawartości ruchu na podstawie wskazanych kryteriów zależnie od funkcjonalności protokołu, który będzie tej filtracji podlegał, np. filtrowanie plików cookies w protokole HTTP. W protokole FTP nie występuje funkcjonalność plików cookie.

ul. Taborowa 33
02-699 Warszawa
tel. 22 601 74 01-03
fax 22 601 74 13
kierownictwo@udsc.gov.pl
www.udsc.gov.pl

Pytanie 3:
Dotyczy opisu wymagań w p. 3 Załącznika nr 1b do SIWZ – Opis Przedmiotu Zamówienia.

Zamawiający określa wymagania funkcje dotyczące filtrowania zawartości ruchu.

- *Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies*

Prosimy o wskazanie czy funkcje filtracji zawartości ruchu HTTP mają dotyczyć również HTTP 2.0 ?

Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że nie ogranicza wymaganych funkcji filtrowania do konkretnej wersji protokołu.

Pytanie 4:

Dotyczy opisu wymagań w p. 3 Załącznika nr 1b do SIWZ – Opis Przedmiotu Zamówienia.

Zamawiający określa w powyższych wymagania funkcje dotyczące deszyfracji ruchu SSL.

- *Urządzenie musi realizować funkcję deszyfrowania ruchu SSL inicjowanego przez użytkowników z wewnątrz chronionej sieci – SSL Forward Proxy. Urządzenie musi inicjować i terminować sesje szyfrowane protokołem SSL w wersjach co najmniej TLS 1.0, TLS 1.1 i TLS 1.2 w oparciu o certyfikaty X.509v3. Na odszyfrowanym ruchu muszą być realizowane funkcje bezpieczeństwa warstwy aplikacyjnej – nie mniej niż dynamiczna identyfikacja aplikacji Web 2.0, IPS, antywirus, URL-filtering. Urządzenie musi pozwalać na wysłanie kopii odszyfrowanego ruchu do zewnętrznego analizatora*

Wykonawca pragnie zauważyć, iż powyższy zestaw wymagań pozwoli Zamawiającemu na niewielkie wykorzystanie podanej funkcji. Wynika to z tego, iż większość serwisów internetowych (niektóre oszacowania wskazują nawet poziom 90%) wykorzystuje już TLS 1.3. Podobnie znajduje to odniesienie dla ruchu SMTP ze STARTTLS.

Prosimy o wyjaśnienie czy funkcja deszyfracji ruchu ma również obejmować SSL w wersji 1.3 oraz deszyfrację ruchu SMTP z wykorzystaniem STARTTLS,w szczególności brak uwzględnienia TLS w wersji 1.3 może wskazywać na omyłkę pisarską.

Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że w specyfikacji określono minimalny poziom wsparcia protokołu SSL z wersjami TLS, tj. TLS 1.0, TLS 1.1, TLS 1.2.
Mając na uwadze powyższe Zamawiający informuje, że TLS w wersji 1.3 spełnia również wymaganie.

Biorąc pod uwagę powyższe, **Zamawiający przedłuża termin składania ofert do dnia 23.11.2020 r. do godz. 12:00. Otwarcie ofert nastąpi w tym samym dniu o godz. 12:15,** w związku z czym:

a) w rozdziale IX pkt 4 ppkt. 1) lit. b) otrzymuje brzmienie:

„b) w postaci papierowego oryginału dokumentu: oryginał dokumentu należy złożyć w oddzielnej kopercie, a jego kopię w ofercie. Dokument należy złożyć **do dnia 23.11.2020 r. do godziny 12:00** w siedzibie Zamawiającego przy ul. Taborowej 33 w Warszawie bezpośrednio w Biurze Podawczym lub przesłać na adres: Urząd do Spraw Cudzoziemców Wydział Zamówień Publicznych **ul. Taborowa 33, 02-699 Warszawa. Z uwagi na zaistniałą sytuację epidemiologiczną, związaną z ogłoszeniem przez Światową Organizację Zdrowia pandemii koronawirusa, zalecane jest przesyłanie ofert poprzez pocztę tradycyjną. Składanie ofert w formie pisemnej w obiekcie Zamawiającego przy ul. Taborowej 33 w**

Warszawie jest możliwe w godz. 08.00 – 09.00 oraz 13.00-14.00 po uprzednim zgłoszeniu telefonicznym pod nr 22 60-154-14.";

b) w rozdziale XI pkt 10 otrzymuje brzmienie:

„10. Ofertę wraz z załącznikami należy umieścić w zamkniętym opakowaniu (kopercie), które należy zaadresować oraz opisać według poniższego wzoru:

Urząd do Spraw Cudzoziemców ul. Taborowa 33, 02-699 Warszawa
OFERTA w postępowaniu na zakup, dostawę i konfigurację urządzeń, licencji oraz zabezpieczeń typu firewall niezbędnych do zapewnienia poprawnego działania oraz zabezpieczenia Modułu Obsługi Spraw Systemu Pobyt v.2 na potrzeby Urzędu do Spraw Cudzoziemców
zadanie częściowe nr ……

Nr sprawy: 24/SYSTEM POBYT V.2-ROZBUDOWA MODUŁU OBSŁUGI SPRAW/PN/20
Otworzyć na jawnym otwarciu ofert w dniu 23.11.2020 r. o godz. 12:15"

c) w rozdziale XII pkt 1 i 4 SIWZ otrzymują brzmienie:

„1. Ofertę w zamkniętym opakowaniu (kopercie) opisanym jak w rozdz. XI pkt 10 SIWZ, należy złożyć **do dnia 23.11.2020 r. do godziny 12:00** w siedzibie Zamawiającego przy ul. Taborowej 33 w Warszawie bezpośrednio w Biurze Podawczym lub przesłać na adres: Urząd do Spraw Cudzoziemców Wydział Zamówień Publicznych **ul. Taborowa 33, 02-699 Warszawa. Z uwagi na zaistniałą sytuację epidemiologiczną, związaną z ogłoszeniem przez Światową Organizację Zdrowia pandemii koronawirusa, zalecane jest przesyłanie ofert poprzez pocztę tradycyjną. Składanie ofert w formie pisemnej w obiekcie Zamawiającego przy ul. Taborowej 33 w Warszawie jest możliwe w godz. 08.00 – 09.00 oraz 13.00-14.00 po uprzednim zgłoszeniu telefonicznym pod nr 22 60-154-14.",**

„4. Otwarcie ofert nastąpi w siedzibie Zamawiającego **przy ul. Taborowej 33 w Warszawie,** w dniu **23.11.2020 r. o godzinie 12:15**.".

Pozostałe zapisy SIWZ nie ulegają zmianie. Zamawiający informuje, że zmiany i wyjaśniania SIWZ są wiążące dla wszystkich Wykonawców biorących udział w przedmiotowym postępowania.

Załączniki:

1. Zmodyfikowany Załącznik nr 1b do Specyfikacji istotnych warunków zamówienia.

ul. Taborowa 33
02-699 Warszawa
tel. 22 601 74 01-03
fax 22 601 74 13
kierownictwo@udsc.gov.pl
www.udsc.gov.pl