Łódź, dnia 10 lipca 2020 r.

EC1/ 613 /2020

DO WSZYSTKICH ZAINTERESOWANYCH
https://platformazakupowa.pl/transakcja/355448

Dotyczy postępowania o udzielenie zamówienia publicznego pn.: ***„Wyposażenie serwerowni Centrum Komiksu i Narracji Interaktywnej"*** **- numer postępowania: 206/DIM/PN/2020**

INFORMACJA
O ZMIANIE TERMINU SKŁADANIA I OTWARCIA OFERT
ORAZ ODPOWIEDZI NA PYTANIA WYKONAWCÓW

Zamawiający „EC1 Łódź - Miasto Kultury" w Łodzi, działając na podstawie art. 38 ust. 4 ustawy z dnia 29 stycznia 2004 roku - Prawo zamówień publicznych (tekst jednolity: Dz.U. 2019 poz. 1843) – dalej ustawa Pzp, **dokonuje modyfikacji treści Specyfikacji Istotnych Warunków Zamówienia (zwanej dalej SIWZ)** w zakresie terminu składania i otwarcia ofert.

I. Zmiana terminu składania i otwarcia ofert (rozdział XIV. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT)):

Zamawiający zmienia termin składania i otwarcia ofert do dzień **27 lipca 2020 r.** Wobec powyższego, treść SIWZ w zakresie pkt. XIV.1. oraz XIV.2. ppkt 1) otrzymuje następujące brzmienie:

„XIV.1. SKŁADANIE OFERT:
Ofertę należy złożyć w formie elektronicznej za pośrednictwem Platformy zakupowej pod adresem: https://platformazakupowa.pl/transakcja/355448
do dnia: ***27 lipca 2020 r. do godziny 12:00"***

oraz

„XIV.2. OTWARCIE OFERT:
1) *Otwarcie ofert nastąpi* ***w dniu 27 lipca 2020 r. o godz. 12:10*** *w siedzibie Zamawiającego przy ul. Tuwima 46 w Łodzi, w Dziale Zamówień Publicznych / Sali konferencyjnej."*

II. Zmiana treści Załącznika nr 1a oraz 1b do SIWZ (OPZ):

Zamawiający dokonuje modyfikacji treści Załącznika nr 1a oraz 1b do SIWZ (Szczegółowy Opis Przedmiotu Zamówienia (OPZ) odpowiednio dla Zadania 1 oraz Zadania 2).
Zmodyfikowany Załącznik nr 1a do SIWZ (OPZ dla Zadania 1) stanowi załacznik nr 2, zaś Załącznik nr 1b do SIWZ (OPZ dla Zadania 2) – załącznik nr 3 do niniejszego pisma.

Pozostałe zapisy SIWZ pozostają bez zmian.

Ponadto Zamawiający, działając na podstawie art. 38 ust. 1 i 2 ustawy Pzp informuje, iż wpłynęły pytania dotyczące treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ), na które udziela następujących wyjaśnień:

Pytanie 1: (Dotyczy Zadania nr 1) Pytanie dot. III.4.4
Czy za równoważne uznane zostanie rozwiązanie pozwalające na osiągnięcie przepustowości dla ruchu VPN IPsec na poziomie 7.8 Gbps przy wykorzystaniu algorytmów AES256-SHA256?

Odpowiedź:
Zamawiający dopuszcza rozwiązanie pozwalające na osiągnięcie przepustowości dla ruchu VPN IPsec na poziomie 7.8 Gbps przy wykorzystaniu algorytmów AES256-SHA256.

Pytanie 2: (Dotyczy Zadania nr 1) Pytanie dot. III.12.1
Czy dopuszczalne jest rozwiązanie wspierające następujące rodzaje plików: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip

Odpowiedź:
Zamawiający, w Załączniku nr 1a do SIWZ (OPZ dla Zadania 1) określił **minimalny** zakres plików, dla których system zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do chmurowego lub lokalnego systemu typu „SandBox". Dopuszczalne jest zaoferowanie rozwiązania, które będzie posiadało szerszą listę takich plików, niemniej jednak obejmującą określony w OPZ zakres minimalny.

Pytanie 3: (Dotyczy Zadania nr 1) Pytanie dot. III.12.2
Czy dopuszczalne jest rozwiązanie które w oparciu o aktualizację sum kontrolnych będących wynikiem działania rozwiązania klasy sandbox jest w stanie zatrzymać przesyłany plik?

Odpowiedź:
Zamawiający podtrzymuje wymaganie określone w pkt. III.12.2 OPZ. W interesie Zamawiającego leży minimalizacja ryzyka związanego z zabezpieczeniem sieci wewnętrznej oraz użytkowników w najlepszy dostępny sposób.

Pytanie 4: (Dotyczy Zadania nr 1) Pytanie dot. III.12.3
Czy dopuszczalne jest rozwiązanie które w związku z integracją z lokalnym systemem plików pozwala na podjęcie decyzji o tym które z nich są przesyłane do lokalnych lub chmurowych systemów typu sandbox?

Odpowiedź:
Zamawiający dopuszcza zaproponowane rozwiązanie, utrzymując jednocześnie wymaganie, iż system typu „Sandbox" musi pochodzić od producenta dostarczonego urządzenia.

Pytanie 5: (Dotyczy Zadania nr 1) Pytanie dot. III.13.2
Czy dopuszczalne jest rozwiązanie które dzięki optymalizacji ilości analizowanego ruchu zwiększa swoją wydajność bez zmniejszenia skuteczności, co zostało potwierdzone w testach niezależnych organizacji certyfikujących?

Odpowiedź:
Zamawiający wymaga, aby ochrona IPS była wykonywana dla całej sesji.

Pytanie 6: (Dotyczy Zadania nr 1) Pytanie dot. III.14.2
Czy dopuszczalne jest rozwiązanie, z rodziny rozwiązań działających w oparciu o dedykowany system operacyjny, które wielokrotnie uzyskiwało rekomendację z ramienia niezależnej organizacji certyfikującej w kategorii NGFW?

Odpowiedź:
Zamawiający nie może odnieść się do powyższego pytania nie znając konkretnego rozwiązania, które proponuje Wykonawca.

Pytanie 7: (Dotyczy Zadania nr 1) Pytanie dot. III.15.1
Czy dopuszczalne jest rozwiązanie wspierające następujące rodzaje plików, nie mniej niż: .net, 7z, activemime, arj, aspack, avi, base64, bat, binhex, bmp, bzip, bzip2, cab, chm, class, cod, crx, dmg, elf, exe, fsg, gif, gzip, hlp, hta, html, iso, jad, javascript, jpeg, lzh, mach-o, mime, mov, mp3, mpeg, msc ,msi, msoffice, msofficex, pdf, petite, png, rar, rm, sis, tar, tiff, torrent, upx, uue, wav, wma, xar, xz, zip?

Odpowiedź:
W ocenie Zamawiającego zaproponowane typy plików nie wyczerpują wszystkich zagrożeń, i ich liczba jest zbyt mała dla oczekiwanego poziomu bezpieczeństwa.
Wobec powyższego Zamawiający podtrzymuje wymaganie określone w pkt. III.15 OPZ.

Pytanie 8: (Dotyczy Zadania nr 1) Pytanie dot. III.18.6
Czy dopuszczalne jest rozwiązanie zapewniające narzędzia takie jak: ping, traceroute, podglądu pakietów, monitorowania stanu i przetwarzania sesji, poszczególnych modułów bezpieczeństwa oraz przetwarzania ruchu przez firewall?

Odpowiedź:
Zamawiający dokonuje modyfikacji treści Załącznika 1a do SIWZ (OPZ dla Zadania 1). Zmodyfikowany OPZ dla Zadania 1 stanowi załącznik do niniejszego pisma.

Pytanie 9: (Dotyczy Zadania nr 1) Pytanie dot. III.19.14
Czy dopuszczalne jest rozwiązanie pozwalające na prezentowanie statystyk ruchu sieciowego które jest dedykowanym systemem logowania, analizy oraz raportowania obsługiwanym z centralnego systemu zarządzania?

Odpowiedź:
Zamawiający nie może odnieść się do powyższego pytania nie znając konkretnego rozwiązania, które proponuje Wykonawca. W pkt. III.19.14 OPZ dla Zadania 1, Zamawiający wskazał minimalne

wymagania, jakie musi spełniać system zarządzania, natomiast w gestii Wykonawcy pozostawia sposób realizacji tych funkcji.

Pytanie 10: (Dotyczy Zadania nr 1) Pytanie dot. III.19.17
Czy dopuszczalne jest rozwiązanie realizujące wspomniane w funkcje w oparciu o dedykowany systemie logowania, analizy oraz raportowania obsługiwanym z centralnego systemu zarządzania?

Odpowiedź:
Zamawiający nie może odnieść się do powyższego pytania nie znając konkretnego rozwiązania, które proponuje Wykonawca. W pkt. III.19.17 OPZ dla Zadania 1, Zamawiający wskazał minimalne wymagania, jakie musi spełniać system zarządzania, natomiast w gestii Wykonawcy pozostawia sposób realizacji tych funkcji.

Pytanie 11: (Dotyczy Zadania nr 1) Pytanie dot. III.20.6
Czy dopuszczalne jest rozwiązanie pozwalające na wykorzystanie ponad 700 zestawień i korelacji danych pozwalających na tworzenie własnych raportów bezpieczeństwa?

Odpowiedź:
Zamawiający dokonuje modyfikacji treści Załącznika 1a do SIWZ (OPZ dla Zadania 1). Zmodyfikowany OPZ dla Zadania 1 stanowi załącznik do niniejszego pisma.

Pytanie 12: (Dotyczy Zadania nr 1) Pytanie dot. III.21.5
Czy dopuszczalne jest rozwiązanie pozwalające na obsługę, przetwarzanie i korelację logów z urządzeń firm trzecich z wykorzystaniem syslog?

Odpowiedź:
Zamawiający podtrzymuje dotychczasowe zapisy OPZ dla Zadania 1 pkt. III.21.5.

Pytanie 13: (Dotyczy Zadania nr 1) Pytanie dot. III.21.7
Czy dopuszczalne jest rozwiązanie pozwalające na automatyczną reakcję w oparciu o: wysłany mail, SNMP, syslog interakcję z systemem firewall.

Odpowiedź:
Zamawiający podtrzymuje dotychczasowe zapisy OPZ dla Zadania 1 pkt. III.21.7.

Pytanie 14: (Dotyczy Zadania nr 1) Pytanie dot. III.21.8
Czy dopuszczalne jest rozwiązanie pozwalające na tworzenie własnych zestawień danych zgromadzonych na systemie logowania?

Odpowiedź:
Zamawiający dopuszcza rozwiązanie pozwalające na tworzenie własnych zestawień danych zgromadzonych na systemie logowania.

Pytanie 15: (Dotyczy Zadania nr 2)
Zostało doprecyzowane pytanie dla odpowiedzi z dnia 30 czerwca. Czy Zamawiający uzna za rozwiązanie równoważne, takie które będzie spełniało poniższe parametry:

propozycja opisu Wykonawcy stanowi załącznik nr 1 do niniejszego pisma.

Odpowiedź Zamawiającego:
Zamawiający dokonuje modyfikacji treści Załącznika 1b do SIWZ (OPZ dla Zadania 2). Zmodyfikowany OPZ dla Zadania 2 stanowi załącznik do niniejszego pisma.

Pytanie 16: Zbiór wymagań dla urządzeń UTM został tak skonstruowany że cały zestaw spełnia tylko jeden producent Checkpoint z urządzeniem Quantum 6200 Next Generation Firewall, w związku z tym czy zamawiający dopuszcza zgodnie z prawem zamówień publicznych inne rozwiązania powyżej wskazany powyżej model. Jeśli tak prosimy o odpowiedź na pytania [*pytania 16 do 26 - przyp. Zamawiającego*] i pozytywne ustosunkowanie się do nich.
Dotyczy zapisów z punktu III.7 Połączenia VPN " Pracę w trybie Tunnel - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki." Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall czy zatem Zamawiający dopuści rozwiązanie realizujące połączenia w trybie Tunnel z wykorzystaniem klienta instalowanego na stacji. Licencje na oprogramowanie klienta vpn nie będą wymagane i nie będą ograniczały ilości osób mogących mieć dostęp do chronionych zasobów.

Odpowiedź:
Zamawiający podtrzymuje wymaganie określone w pkt. III.7 OPZ.
Jednocześnie Zamawiający pragnie zauważyć, że powyższy zapis nie wskazuje na żadne konkretne urządzenie. Zamawiający dokonując opisu przedmiotu zamówienia miał na uwadze funkcje opisywanego systemu a nie urządzenia, stąd przede wszystkim wskazywał na wymagane i niezbędne funkcjonalności. Opisane funkcjonalności mają na celu zwiększenie bezpieczeństwa i stopnia ochrony systemów informatycznych, jednostek komputerowych znajdujących się w posiadaniu Zamawiającego oraz użytkowników końcowych. W tym, względzie opis przedmiotu zamówienia jest zgody z przepisami Prawa zamówień publicznych. W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 17:
Dotyczy zapisów z punktu III.8 Routing i obsługa łączy WAN " System musi umożliwiać sterowaniem ruchem dla co najmniej 2 łączy WAN poprzez reguły PBR (Policy Base Routing), w których można wykorzystać zdefiniowane reguły z polityki bezpieczeństwa na FW." Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall czy zatem zamawiający dopuści rozwiązanie które będzie umożliwiać sterowaniem ruchem dla co najmniej 2 łączy WAN poprzez reguły PBR (Policy Base Routing), oraz budować polityki bezpieczeństwa na FW dla tego ruchu".

Odpowiedź:
Zamawiający podtrzymuje wymaganie określone w pkt. III.8 OPZ.
Jednocześnie Zamawiający pragnie zauważyć, że powyższy zapis nie wskazuje na żadne konkretne urządzenie. Zamawiający dokonując opisu przedmiotu zamówienia miał na uwadze funkcje opisywanego systemu a nie urządzenia, stąd przede wszystkim wskazywał na wymagane i niezbędne funkcjonalności. Opisane funkcjonalności mają na celu zwiększenie bezpieczeństwa i stopnia ochrony systemów informatycznych, jednostek komputerowych znajdujących się w posiadaniu

Zamawiającego oraz użytkowników końcowych. W tym, względzie opis przedmiotu zamówienia jest zgody z przepisami Prawa zamówień publicznych. W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 18:
Dotyczy zapisów z punktu III.12 Ochrona typu Sandbox: „System zabezpieczeń firewall musi posiadać funkcję, zatrzymania pliku na urządzeniu do momentu wydania werdyktu przez system typu „SandBox". Nie dopuszczalne jest, aby plik transportowany z Internetu do użytkownika miałby możliwość pojawienia się na urządzeniu bez otrzymania werdyktu o pliku." Ze względu na to że czas analizy pliku w środowiskach enterprise przy dużym natężeniu ruchu i dużej ilości plików może być długi w rozwiązaniach klasy enterprise nie stosuje się wstrzymywania sesji do otrzymania efektu z analizy. Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall czy zatem Zmawiający zezwoli na dostarczenie rozwiązania, które nie posiada funkcji zatrzymywania pliku do czasu przeanalizowania go przez rozwiązania SandBox?

Odpowiedź:
Zamawiający podtrzymuje wymaganie określone w pkt. III.12 OPZ.
Zamawiający nie może odnieść się do powyższego pytania nie znając konkretnego rozwiązania, które proponuje Wykonawca. W interesie Zamawiającego leży minimalizacja ryzyka związanego z zabezpieczeniem sieci wewnętrznej oraz użytkowników w najlepszy dostępny sposób.
W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 19:
Dotyczy zapisów z punktu III.13 Ochrona przed atakami: „System powinien posiadać mechanizm automatycznego dodawania adresu IP do czarnej listy (z ang. Black list) w przypadku spełnienia warunku naruszenia zasad bezpieczeństwa wykrytych przez moduł IPS/IDS." Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall czy zatem Zamawiający dopuści mechanizm kwarantanny zamiast czarnej listy?

Odpowiedź:
Zamawiający dopuszcza zaproponowane rozwiązanie.
Jednocześnie Zamawiający pragnie zauważyć, że powyższy zapis nie wskazuje na żadne konkretne urządzenie. Zamawiający dokonując opisu przedmiotu zamówienia miał na uwadze funkcje opisywanego systemu a nie urządzenia, stąd przede wszystkim wskazywał na wymagane i niezbędne funkcjonalności. Opisane funkcjonalności mają na celu zwiększenie bezpieczeństwa i stopnia ochrony systemów informatycznych, jednostek komputerowych znajdujących się w posiadaniu Zamawiającego oraz użytkowników końcowych. W tym, względzie opis przedmiotu zamówienia jest zgody z przepisami Prawa zamówień publicznych. W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 20:
Dotyczy zapisów z punktu III.14 Kontrola aplikacji: „System musi zapewniać bazę kontroli aplikacji, która powinna zawierać minimum 7500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora." Zapis wskazuje na Checkpoint Quantum

6200 Next Generation Firewall czy zatem Zamawiający dopuści rozwiązanie posiadające 2300 sygnatur?

Odpowiedź:
Zamawiający podtrzymuje wymaganie określone w pkt. III.14 OPZ.
Jednocześnie Zamawiający pragnie zauważyć, że powyższy zapis nie wskazuje na żadne konkretne urządzenie. Zamawiający dokonując opisu przedmiotu zamówienia miał na uwadze funkcje opisywanego systemu a nie urządzenia, stąd przede wszystkim wskazywał na wymagane i niezbędne funkcjonalności. Opisane funkcjonalności mają na celu zwiększenie bezpieczeństwa i stopnia ochrony systemów informatycznych, jednostek komputerowych znajdujących się w posiadaniu Zamawiającego oraz użytkowników końcowych. W tym, względzie opis przedmiotu zamówienia jest zgody z przepisami Prawa zamówień publicznych. W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 21:
Dotyczy zapisów z punktu III.15 Kontrola przepływu danych: „System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików w obu kierunkach, nie mniej niż: bat, cab, dll, doc, szyfrowany zip, docx, xlsx, pptx, pdf, jpg, jpeg, exe, com, dll, drv, pif, qts, qtx, sys, scr, vbx, vxd, gif, png, tiff, asf, wmv, wma, mp3, 7f, mdb, accdb, dbf, db, ras, bmp, xpm, psd, ps, dwg, rtf, rar, gz, tgz, tar.gz, tar.z, bz2, tar.bz2, tbz2, tb2, jar, lha, lzh, arc, kgb, xy, reg, rpm, arj, bh, zoo, cpio, ace, deb, avi, wmf, rm, rv, emf, pbm, pgm, ppm, gem, xml, doc, ppt, xls, swf, mov, mp4, mpeg, flv, dwf, mkv, js, css, wav, pak, tar, mdg, oft, eml, pst, odt, ott, ods, ots, odg , otg, odp, otp, odi, oti, ico, wks, wk1, wk2, wk3, wk4, wk5, 123, dxf, hwp, one, webp, Zip (compressed using BZip2), Zip (compressed using Deflate64), Zip (compressed using LZMA), Zip (compressed using PPMD), html, xhtml, phtml, htm. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka, a nie na podstawie rozszerzenia."
Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall czy zatem Zamawiający dopuści rozwiązanie pozwalające na blokownie transmisji plików „7z, arj, cab, lzh, rar, tar, zip, bzip, gzip, bzip2, xz, bat, msc, uue, mime, base64, binhex, elf, exe, hta, html, jad, class, cod, javascript, msoffice, msofficex, fsg, upx, petite, aspack, sis, hlp, activemime, jpeg, gif, tiff, png, bmp, unknown, mpeg, mov, mp3, wma, wav, pdf, avi, rm, torrent, msi, mach-o, dmg, .net, xar, chm, iso, crxflac"?

Odpowiedź:
W ocenie Zamawiającego zaproponowane typy plików nie wyczerpują wszystkich zagrożeń, i ich liczba jest zbyt mała dla oczekiwanego poziomu bezpieczeństwa.
Wobec powyższego Zamawiający podtrzymuje wymaganie określone w pkt. III.15 OPZ.
Jednocześnie Zamawiający pragnie zauważyć, że powyższy zapis nie wskazuje na żadne konkretne urządzenie. Zamawiający dokonując opisu przedmiotu zamówienia miał na uwadze funkcje opisywanego systemu a nie urządzenia, stąd przede wszystkim wskazywał na wymagane i niezbędne funkcjonalności. Opisane funkcjonalności mają na celu zwiększenie bezpieczeństwa i stopnia ochrony systemów informatycznych, jednostek komputerowych znajdujących się w posiadaniu Zamawiającego oraz użytkowników końcowych. W tym, względzie opis przedmiotu zamówienia jest zgody z przepisami Prawa zamówień publicznych. W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 22:
Dotyczy zapisów z punktu III.17 Zarządzenie tożsamością użytkowników – uwierzytelnienie użytkowników w ramach sesji:" System zabezpieczeń firewall musi odczytywać oryginalne adresy IP

stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesję, w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia." Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall czy zatem Zamawiający dopuści rozwiązanie nie posiadające tej funkcjonalności a realizujące rozpoznawanie użytkowników poprzez klienta do kontrolerów ActiveDirectory, lub realizującego funkcjonalność proxy w ramach funkcjonalności UTM?

Odpowiedź:
Zamawiający podtrzymuje wymaganie określone w pkt. III.17 OPZ.
Jednocześnie Zamawiający pragnie zauważyć, że powyższy zapis nie wskazuje na żadne konkretne urządzenie. Zamawiający dokonując opisu przedmiotu zamówienia miał na uwadze funkcje opisywanego systemu a nie urządzenia, stąd przede wszystkim wskazywał na wymagane i niezbędne funkcjonalności. Opisane funkcjonalności mają na celu zwiększenie bezpieczeństwa i stopnia ochrony systemów informatycznych, jednostek komputerowych znajdujących się w posiadaniu Zamawiającego oraz użytkowników końcowych. W tym, względzie opis przedmiotu zamówienia jest zgody z przepisami Prawa zamówień publicznych. W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 23:
Dotyczy zapisów z punktu III.17 Zarządzenie tożsamością użytkowników – uwierzytelnienie użytkowników w ramach sesji:" Urządzenie musi posiadać funkcjonalność współdzielenia tożsamości między systemami firewall pochodzącymi od tego samego producenta, jednakże zarządzanymi poprzez odrębne domeny zarządzania." Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall czy zatem Zamawiający dopuści rozwiązanie które posiada Agenta po stronie serwerów Active directory które może przekazywać informacje o tożsamości użytkowników do wielu urządzeń tego samego producenta?

Odpowiedź:
Zamawiający podtrzymuje wymaganie określone w pkt. III.17 OPZ.
Jednocześnie Zamawiający pragnie zauważyć, że powyższy zapis nie wskazuje na żadne konkretne urządzenie. Zamawiający dokonując opisu przedmiotu zamówienia miał na uwadze funkcje opisywanego systemu a nie urządzenia, stąd przede wszystkim wskazywał na wymagane i niezbędne funkcjonalności. Opisane funkcjonalności mają na celu zwiększenie bezpieczeństwa i stopnia ochrony systemów informatycznych, jednostek komputerowych znajdujących się w posiadaniu Zamawiającego oraz użytkowników końcowych. W tym, względzie opis przedmiotu zamówienia jest zgody z przepisami Prawa zamówień publicznych. W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 24:
Dotyczy zapisów z punktu III.18 Zarządzanie Systemem Firewall: „Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, hping, hping2, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall." Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall czy zatem Zamawiający dopuści rozwiązanie które posiada narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Odpowiedź:
Zamawiający dokonuje modyfikacji treści Załącznika 1a do SIWZ (OPZ dla Zadania 1). Zmodyfikowany OPZ dla Zadania 1 stanowi załącznik do niniejszego pisma.

Pytanie 25:
Dotyczy zapisów z punktu III.19 Serwer zarządzania – wymagania ogólne: „Serwer zarządzania musi posiadać mechanizmy pozwalające na weryfikację poprawności działania nowej wersji polityki bezpieczeństwa po jej uruchomieniu na zaporze sieciowej oraz możliwość automatycznego powrotu do poprzedniej wersji w przypadku stwierdzenia nieprawidłowości na bazie zestawu testów utworzonych przez administratora - np. brak dostępu do wybranych usług powstały w wyniku błędu administratora." Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall wraz z Unified Security Management czy zatem Zamawiający zrezygnuje z tego wymagania?

Odpowiedź:
Zamawiający podtrzymuje wymaganie określone w pkt. III.19 OPZ.
Jednocześnie Zamawiający pragnie zauważyć, że powyższy zapis nie wskazuje na żadne konkretne urządzenie. Zamawiający dokonując opisu przedmiotu zamówienia miał na uwadze funkcje opisywanego systemu a nie urządzenia, stąd przede wszystkim wskazywał na wymagane i niezbędne funkcjonalności. Opisane funkcjonalności mają na celu zwiększenie bezpieczeństwa i stopnia ochrony systemów informatycznych, jednostek komputerowych znajdujących się w posiadaniu Zamawiającego oraz użytkowników końcowych. W tym, względzie opis przedmiotu zamówienia jest zgody z przepisami Prawa zamówień publicznych. W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 26:
Dotyczy zapisów z punktu III.21 Serwer zarządzania - logi, zdarzenia, korelacja „Serwer zarządzania musi zapewniać obsługę przechowywania zdarzeń, przetwarzania i korelację logów z urządzeń firm trzecich, z wykorzystaniem co najmniej Syslog i SNMP." Zapis wskazuje na Checkpoint Quantum 6200 Next Generation Firewall wraz z Unified Security Management czy zatem Zamawiający dopuści rozwiązanie spełniające wymaganie „Serwer zarządzania musi zapewniać obsługę przechowywania zdarzeń, przetwarzania i korelację logów z urządzeń firm trzecich, z wykorzystaniem co najmniej Syslog."?

Odpowiedź:
Zamawiający podtrzymuje wymaganie określone w III.21.
Jednocześnie Zamawiający pragnie zauważyć, że powyższy zapis nie wskazuje na żadne konkretne urządzenie. Zamawiający dokonując opisu przedmiotu zamówienia miał na uwadze funkcje opisywanego systemu a nie urządzenia, stąd przede wszystkim wskazywał na wymagane i niezbędne funkcjonalności. Opisane funkcjonalności mają na celu zwiększenie bezpieczeństwa i stopnia ochrony systemów informatycznych, jednostek komputerowych znajdujących się w posiadaniu Zamawiającego oraz użytkowników końcowych. W tym, względzie opis przedmiotu zamówienia jest zgody z przepisami Prawa zamówień publicznych. W ocenie Zamawiającego na rynku istnieje więcej niż jedno rozwiązanie spełniające postawiony warunek.

Pytanie 27:
Dotyczy zapisów z punktu 4. Przełączniki LAN 10Gbps. Czy Zamawiający dopuści przełącznik nie mający możliwości montażu w szafie dwóch przełączników koło siebie, ale za to pozwalający na rozbudowę do 24 portów SFP+ w ramach jednego przełącznika 1U?

Odpowiedź:
Zamawiający dopuszcza zaproponowane rozwiązanie pozwalające na rozbudowę do 24 portów SFP+ w ramach jednego przełącznika 1U.
Zamawiający dokonuje modyfikacji treści Załącznika 1b do SIWZ (OPZ dla Zadania 2) w zakresie montażu przełączników obok siebie. Zmodyfikowany OPZ dla Zadania 2 stanowi załącznik do niniejszego pisma.

Pytanie 28:
Dotyczy zapisów z punktu 4. Przełączniki LAN 10Gbps. Czy Zamawiający dopuści przełącznik posiadający dożywotnią, nie ograniczoną czasowo gwarancję z czasem wysyłki na następny dzień roboczy od przyjęcia zgłoszenia z możliwością zgłaszania usterek w trybie 24x7 poprzez portal WWW oraz telefonicznie w trybie 8x5?

Odpowiedź:
Zamawiający dopuszcza zaproponowane rozwiązanie.
Zamawiający dokonuje modyfikacji treści Załącznika 1b do SIWZ (OPZ dla Zadania 2) w zakresie trybu zgłaszania awarii. Zmodyfikowany OPZ dla Zadania 2 stanowi załącznik do niniejszego pisma.

Pytanie 29:
Dotyczy zapisów z punktu 4. Przełączniki LAN 10Gbps. Czy Zamawiający dopuści przełączniki posiadające maksymalny pobór mocy do 120W ale za to posiadający 16 portów SFP+ z dalszą możliwością rozbudowy i stackowaniem?

Odpowiedź:
Zamawiający, pismem z dnia 30 czerwca 2020 r. (EC1/579/2020), dokonał modyfikacji Załącznika 1b do SIWZ (OPZ dla Zadania 2) w zakresie maksymalnego poboru mocy.
Zamawiający nie stawia wymogu co do dalszej rozbudowy i stackowania.

Pytanie 30:
Dotyczy zapisów z punktu 4. Przełączniki LAN 10Gbps. Czy Zamawiający dopuści przełączniki pracujące w zakresie temperatur od 0 do 45 stopni Celsjusza?

Odpowiedź:
Zamawiający dopuszcza zaproponowane rozwiązanie.
Zamawiający, pismem z dnia 30 czerwca 2020 r. (EC1/579/2020), dokonał modyfikacji Załącznika 1b do SIWZ (OPZ dla Zadania 2) w zakresie temperatury pracy przełączników.

Pytanie 31:
Dotyczy zapisów z punktu 4. Przełączniki LAN 10Gbps. Czy Zamawiający dopuści przełączniki posiadające zaawansowane funkcje zarządzania jakością QoS jednak bez wsparcia dla WRR?

Odpowiedź:
Zamawiający dopuszcza zaproponowane rozwiązanie.
Zamawiający dokonuje modyfikacji treści Załącznika 1b do SIWZ (OPZ dla Zadania 2) w zakresie zarządzania siecią i bezpieczeństwa. Zmodyfikowany OPZ dla Zadania 2 stanowi załącznik do niniejszego pisma.

Pytanie 32:
Dotyczy zapisów z punktu 4. Przełączniki LAN 10Gbps. Przełączniki agregujące połączenia 10Gb, takie jak opisane w tym punkcie, ze względu na swoją specyfikę i krytyczne umiejscowienie w sieci powinny mieć modularne i redundantne krytyczne elementy takie jak zasilacze i wentylatory, aby awaria zasilania lub wentylacji (czyli elementów najbardziej narażonych na awarię), nie powodowała awarii całego segmentu sieci. Jest to tym bardziej krytyczne jeżeli przełącznik agreguje połączenia do serwerów i macierzy. Czy Zamawiający wymaga by wentylatory i zasilacze były modularne? Czy przełącznik powinien być dostarczony z jednym czy dwoma zasilaczami?

Odpowiedź:
Zamawiający nie wymaga, aby zasilacze i wentylatory były modularne. Zamawiający nie stawia również wymogu w zakresie redundancji zasilaczy.

Pytanie 33:
Dotyczy zapisów z punktu 4. Przełączniki LAN 10Gbps. Czy Zamawiający zgadza się na rezygnację z wymagania szablonów konfiguracji portów?

Odpowiedź:
Zamawiający dopuszcza zaproponowane rozwiązanie.
Zamawiający dokonuje modyfikacji treści Załącznika 1b do SIWZ (OPZ dla Zadania 2) w zakresie zarządzania siecią i bezpieczeństwa. Zmodyfikowany OPZ dla Zadania 2 stanowi załącznik do niniejszego pisma.

Pytanie 34:
Dotyczy zapisów z punktu 4. Przełączniki LAN 10Gbps. Czy Zamawiający poprzez „kabel SFP, 1000BASE-T" rozumie wkładkę SFP 1000Base-T?

Odpowiedź:
Zamawiający, pismem z dnia 30 czerwca 2020 r. (EC1/579/2020), dokonał modyfikacji Załącznika 1b do SIWZ (OPZ dla Zadania 2) w ww. zakresie.

Pytanie 35:
Dotyczy Zadania nr 1. Treść: III.19.19 „Musi istnieć możliwość zarządzania wieloma domenami. Musi istnieć możliwość utworzenia co najmniej 5 domen administracyjnych na podstawie położenia geograficznego, jednostki biznesowej lub funkcji bezpieczeństwa (licencja musi być częścią oferty)." Pytanie[do zadania 1]: Czy zamawiający zaakceptuje rozwiązanie pozwalające na zarządzanie 5 niezależnymi systemami NGFW w ramach jednej domeny administracyjnej? Wydzielenie administracyjne będzie realizowane na podstawie konfiguracji dostępu (Role Base Administration)?

Odpowiedź:

Zamawiający dopuszcza zaproponowane rozwiązanie.
Zamawiający dokonuje modyfikacji treści Załącznika 1a do SIWZ (OPZ dla Zadania 1) w zakresie zarządzania siecią i bezpieczeństwa. Zmodyfikowany OPZ dla Zadania 1 stanowi załącznik do niniejszego pisma.

Zamawiający informuje, iż niniejsze odpowiedzi na pytania (wraz z załącznikami) stanowią integralną część SIWZ i dokumentację postępowania.

Załączniki do niniejszego pisma:
Załącznik nr 1 – propozycja opisu Wykonawcy dla Zadania 2
Załącznik nr 2 – Opis przedmiotu zamówienia dla Zadania 1 (Załącznik nr 1a do SIWZ) po modyfikacji z dnia 10 lipca 2020 r.
Załącznik nr 3 – Opis przedmiotu zamówienia dla Zadania 2 (Załącznik nr 1b do SIWZ) po modyfikacji z dnia 10 lipca 2020 r.

Z upoważnienia
Dyrektora

Joanna Zielecka-Lewicz
Kierownik Działu
Zamówień Publicznych