
**UNIWERSYTET KAZIMIERZA WIELKIEGO**

1. **W BYDGOSZCZY**
2. ul. Chodkiewicza 30, 85 – 064 Bydgoszcz, tel. 052 341 91 00 fax. 052 360 82 06
3. NIP 5542647568 REGON 340057695
4. www.ukw.edu.pl

UKW/DZP-281-D-77/2018 Bydgoszcz, dn. 29.11. 2018 r.

# dot. postępowania prowadzonego w trybie przetargu nieograniczonego na: Dostawa urządzenia bezpieczeństwa sieciowego – typu next generation firewall oraz oprogramowania zabezpieczającego stacje końcowe

**ODPOWIEDZI NA PYTANIA**

#  Działając na podstawie art. 38 ust. 1 ustawy Prawo zamówień publicznych (tj. Dz. U. z 2018 r. poz. 1986) Zamawiający przekazuje treść zapytań wraz z udzielonymi odpowiedziami w postępowaniu o udzielenie zamówienia publicznego na: Dostawę urządzenia bezpieczeństwa sieciowego – typu next generation firewall oraz oprogramowania zabezpieczającego stacje końcowe”:

**Pytanie 1**

Dotyczy: Część 1 - Urządzenie bezpieczeństwa sieciowego – UTM:

SIWZ Część 1 – punkt „System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (urządzenie fizyczne, zamawiający nie dopuszcza rozwiązania w formie maszyny wirtualnej). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta”

**Pytanie**: Czy zamawiający dopuści rozwiązanie w formie maszyny fizycznej, w którym separacja modułu zarządzania i przetwarzania danych będzie się odbywała w formie logicznej?

**Uzasadnienie**: Zastosowanie zmiany będzie miało wpływ na większą liczbę oferentów oraz korzystnie wpłynie na obniżenie ceny zakupu.

**Odp. Zamawiający dopuszcza rozwiązanie, w którym separacja danych będzie się odbywała w formie logicznej.**

**Pytanie 2**

SIWZ Część 1 – punkt „Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.)”

**Pytanie**: Czy zamawiający zaakceptuje rozwiązanie równoważne pod względem trybów konfigurowalnych w inny sposób? Np. konfiguracja per cały wirtualny system, konfiguracja L2 per para interfejsów w ramach systemu wirtualnego L3?

**Uzasadnienie**: Powyższe wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Zastosowanie zmiany będzie miało wpływ na większą liczbę oferentów oraz korzystnie wpłynie na obniżenie ceny zakupu.

**Odp. Zamawiający dopuszcza zaproponowane rozwiązanie równoważne.**

**Pytanie 3**

SIWZ Część 1 – punkt „System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN”

**Pytanie**: Czy zamawiający dopuści rozwiązanie, które w ramach jednej instancji będzie obsługiwało 1024 znaczniki vlan, natomiast 4096 znaczników będzie mogło być obsłużone w ramach sumy kilku instancji wirtualnych?

**Uzasadnienie**: W opisie zamówienia widnieje informacja – „Urządzenie musi obsługiwać 4094 znaczników VLAN”, która jest niejednoznaczna przy wymaganiu systemu z instancjami wirtualnymi.

**Odp. Zamawiający dopuszcza zaproponowane rozwiązanie.**

**Pytanie 4**

SIWZ Część 1 – punkt „System zabezpieczeń firewall musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF;”

**Pytanie**: Czy zamawiający zaakceptuje rozwiązanie posiadające oddzielną tablicę routingu per system wirtualny?

**Uzasadnienie**: Powyższe wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Zastosowanie zmiany będzie miało wpływ na większą liczbę oferentów oraz korzystnie wpłynie na obniżenie ceny zakupu.

**Odp. W ocenie zamawiającego powyższy zapis dopuszcza taką możliwość. Należy zwrócić szczególnie uwagę na wymóg możliwości uruchomienia więcej niż jednej tablicy routingu dla pojedynczej instancji systemu zabezpieczeń.**

**Pytanie 5**

SIWZ Część 1 – punkt „Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM)”

**Pytanie:** Czy zamawiający zezwala na rozwiązanie równoważne, w którym konfiguracja portów i definiowania aplikacji będzie odbywać się w innym miejscu niż reguła firewall. Reguła firewall będzie miała możliwość wybrania zdefiniowanych elementów.

**Uzasadnienie:** Powyższe wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Zastosowanie zmiany będzie miało wpływ na większą liczbę oferentów oraz korzystnie wpłynie na obniżenie ceny zakupu.

**Odp. Zamawiający dopuszcza zaproponowane rozwiązanie równoważne.**

**Pytanie 6**

SIWZ Część 1 – punkt „System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta”

**Pytanie:** Czy zamawiający zezwala na rozwiązanie równoważne, w którym tworzenie sygnatur dla nowych aplikacji będzie możliwe przy użyciu zewnętrznych narzędzi?

**Uzasadnienie:** Powyższe wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Zastosowanie zmiany będzie miało wpływ na większą liczbę oferentów oraz korzystnie wpłynie na obniżenie ceny zakupu.

**Odp. Zamawiający zezwala na tworzenie sygnatur przy użyciu zewnętrznych narzędzi , pod warunkiem, że narzędzia te nie są pozycjami dodatkowo płatnymi (np. dostępnymi w ramach osobnej płatnej subskrypcji / licencji). Oferowane narzędzie będzie oficjalnym edytorem polecanym przez producenta.**

**Pytanie 7**

SIWZ Część 1 – punkt „System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie”

**Pytanie 1**: Czy zamawiający przez AS rozumie zagrożenia typu Spyware?

**Pytanie 2**: Jeżeli odpowiedź na pytanie 1 jest twierdząca, czy zamawiający dopuszcza usunięcie zapisu AS z opisu przedmiotu zamówienia?

**Uzasadnienie**: Ponieważ znacząca większość producentów nie rozróżnia osobnych profili bezpieczeństwa dla zagrożeń typu „spyware”, jest to typowe rozdzielenie dla producenta Palo Alto Networks. Dodatkowo warto zwrócić uwagę, że zagrożenia typu „spyware” są zawarte w sygnaturach antywirusowych i mogą być wykrywane i blokowane za pomocą tychże profili.

**Odp 1. Zamawiający przez AS rozumie Anty-spyware.**

**Odp. 2. Zamawiający nie usunie zapisu „AS”. Urządzenie ma wykrywać tego typu zagrożenia. Zamawiający natomiast dopuszcza możliwość integracji profilu AS z innym zbieżnym profilem, jeżeli Wykonawca wykaże funkcjonalność faktycznego wykrywania zagrożeń typu spyware przez oferowany produkt, z przedstawieniem konkretnych wektorów ataków i skutecznie wykrytego spyware, zgodnie z danymi producenta. Połączony profil (kontekst) AS z innym profilem, musi umożliwiać w ramach połączonego profilu definicję wyłącznie reagowania na zagrożenia typu spyware oraz raportowania takiej (osobnej) kategorii w ramach systemu logowania / raportowania zdarzeń.**

**Uwaga: Zamawiający nie przywiązuje konkretnej wagi do nazewnictwa AV, AS, IPS pod warunkiem, że Wykonawca jest w stanie logicznie oddzielić te kategorie w taki sposób by umożliwić przejrzyste raportowanie per dana kategoria i umożliwić budowanie skutecznych polityk i reguł bezpieczeństwa. Ideą Zamawiającego nie jest wskazanie konkretnych produktów tylko przyjęcie konkretnych powszechnych taksonomi.**

**Pytanie 8**

SIWZ Część 1 – „System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików”

**Pytanie**: Czy zamawiający dopuści usunięcie lub zmianę zapisu na następujące, aby dopuści rozwiązania równoważne i konkurencyjne do opisanego: „System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download”

**Uzasadnienie**: Zamawiający wymaga, aby rozwiązanie firewall zapewniało ochronę przed atakami „Drive-by-Download” w sposób wspierany tylko przez jednego producenta (Palo Alto Networks) i dodatkowo nie gwarantujący tej ochrony i pozostawiający użytkownikowi decyzyjność w sprawie blokowania danego pliku

**Odp. Zamawiający zmieni zapis na „System zabezpieczeń firewall powinien zapewniać ochronę przed atakami typu „Drive-by-download” i zmodyfikuje treść SIWZ w tym zakresie.**

**Pytanie 9**

SIWZ Część 1 – „System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH”

**Pytanie**: Czy zamawiający zaakceptuje rozwiązanie wykonujące inspekcję ruchu SSH pod kątem funkcji Exec, Port-Forward, SSH-Shell, X11-Filter?

**Uzasadnienie:** Powyższe wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Zastosowanie zmiany będzie miało wpływ na większą liczbę oferentów oraz korzystnie wpłynie na obniżenie ceny zakupu.

**Odp. Zamawiający wymaga aby urządzenie zapewniało pełną inspekcję ruchu SSH.**

**Pytanie 10**

SIWZ Część 1 – „System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL”

**Pytanie**: Czy wymaganie dotyczy inspekcji ruchu SMTP zaszyfrowanego za pomocą SSL? Jakiego rodzaju ruch poza http będzie poddany rozszyfrowaniu i inspekcji?

**Uzasadnienie:** Usunięcie wymagania będzie miało wpływ na większą liczbę oferentów oraz korzystnie wpłynie na obniżenie ceny zakupu.

**Odp. Oferowane rozwiązanie poza inspekcją ruchu szyfrowanego HTTPS musi umożliwiać rozszywanie sesji szyfrowanej dla następujących protokółów: IMAP(S), POP3(S), SMTP(S), FTP(S) .**

**Pytanie 11**

SIWZ Część 1 – „System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników”

**Pytanie**: Czy zamawiający dopuszcza integrację z zewnętrznym systemem w ramach zapewnienia ww. funkcjonalności.

**Uzasadnienie**: Zamawiający wymaga aby rozwiązanie mogło analizować logi syslog i odzwierciedlać na tej podstawie adresy IP użytkowników w polityce bezpieczeństwa. Ponieważ analiza logów, zwłaszcza w dużych środowiskach wymaga wydzielonych zasobów (poza urządzeniem firewall), wnosimy o dopuszczenie zewnętrznych rozwiązań w formie maszyny wirtualnej zintegrowanej z rozwiązaniem firewall i dostarczającej wymaganej funkcjonalności.

**Odp. Zamawiający dopuszcza dodatkowe rozwiązanie w formie maszyny wirtualnej lub maszyny fizycznej, które nie będzie wymagało zakupu dodatkowych licencji/subslrypcji, ani nie będzie miało wpływ na koszty wsparcia (nie będzie osobno wycenionym produktem, generującym dodatkowy koszt).**

**Pytanie 12**

SIWZ Cześć 1 – „System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa)”

**Pytanie**: Czy zamawiający dopuszcza równoważny sposób realizacji ochrony filtrowania stron WWW?

**Uzasadnienie**: Sugerowany sposób realizacji blokowania stron WWW uniemożliwia zastosowanie rozwiązań wielu producentów, których sposób realizacji blokowania stron jest równie skuteczny do wskazanego w opisywanym punkcie.

**Odp. Zamawiający dopuszcza rozwiązanie równoważne, jednak nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per całe urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).**

**Pytanie 13**

SIWZ Cześć 1 – „System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa)”

**Pytanie**: Czy zamawiający dopuszcza równoważny sposób realizacji ochrony antywirusowej?

**Uzasadnienie**: Sugerowany sposób realizacji ochrony antywirusowej uniemożliwia zastosowanie rozwiązań wielu producentów, których sposób realizacji tego zadania jest równie skuteczny do wskazanego w opisywanym punkcie.

**Odp. Zamawiający dopuszczamy rozwiązanie równoważne, jednak nie jest dopuszczalne, aby funkcja ochrony antywirusowej uruchamiana była per całe urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).**

**Pytanie 14**

SIWZ Cześć 1 – „System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa);

**Pytanie**: Czy zamawiający dopuszcza równoważny sposób realizacji ochrony IPS/IDS?

**Uzasadnienie**: Sugerowany sposób realizacji ochrony IPS/IDS uniemożliwia zastosowanie rozwiązań wielu producentów, których sposób realizacji tego zadania jest równie skuteczny do wskazanego w opisywanym punkcie.

**Odp. Zamawiający dopuszcza rozwiązanie równoważne, jednak nie jest dopuszczalne, aby sposób realizacji ochrony IPS/IDS uruchamiana była per całe urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).**

**Pytanie 15**

SIWZ Część 1 – punkt „System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta”

**Pytanie:** Czy zamawiający zezwala na rozwiązanie równoważne, w którym tworzenie sygnatur IPS będzie możliwe przy użyciu zewnętrznych narzędzi?

**Uzasadnienie:** Powyższe wymaganie sugeruje zastosowanie rozwiązania konkretnego producenta. Zastosowanie zmiany będzie miało wpływ na większą liczbę oferentów oraz korzystnie wpłynie na obniżenie ceny zakupu.

**Odp. Zamawiający zezwala na tworzenie sygnatur przy użyciu zewnętrznych narzędzi , pod warunkiem, że narzędzia te nie są pozycjami dodatkowo płatnymi (np. dostępnymi w ramach osobnej płatnej subskrypcji / licencji). Oferowane narzędzie będzie oficjalnym edytorem polecanym przez producenta.**

**Pytanie 16**

SIWZ Część 1 – punkt „System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny” oraz

„System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa)” oraz

„System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta”

**Pytanie**: Czy zamawiający dopuszcza usunięcie powyższego zapisu z opisu przedmiotu zamówienia.

**Uzasadnienie**: Większość producentów nie rozróżnia osobnych profili bezpieczeństwa dla zagrożeń typu „spyware”, jest to typowe rozdzielenie dla producenta Palo Alto Networks. Dodatkowo warto zwrócić uwagę, że zagrożenia typu „spyware” są zawarte w sygnaturach antywirusowych i mogą być wykrywane i blokowane za pomocą tychże profili.

**Odp. Odpowiedzi zostały udzielone do poszczególnych fragmentów cytowanych przez Wykonawcę zapisów SIWZ.**

**Dot. SIWZ Część 1 – punkt „System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny” oraz**

**Odpowiedź: Zamawiający dopuszcza możliwość integracji profilu AS z innym zbieżnym modułem, realizującym np. ochronę antywirus, jeżeli Wykonawca wykaże funkcjonalność faktycznego wykrywania zagrożeń typu spyware przez oferowany produkt, z przedstawieniem konkretnych wektorów ataków i skutecznie wykrytego spyware, zgodnie z danymi producenta. Połączona funkcjonalność AS z inną (np. AV), musi umożliwiać w ramach takiego połączenia definicję wyłącznie reagowania na zagrożenia typu spyware oraz raportowania takiej (osobnej) kategorii w ramach systemu logowania / raportowania zdarzeń.**

**Dot. „System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa)” oraz**

**Odpowiedź: Zamawiający dopuszcza rozwiązanie równoważne, jednak nie jest dopuszczalne, aby taka funkcjonalność uruchamiana była per całe urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).**

**Dot. „System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta”**

**Odpowiedź: Zamawiający zezwala na tworzenie sygnatur przy użyciu zewnętrznych narzędzi , pod warunkiem, że narzędzia te nie są pozycjami dodatkowo płatnymi (np. dostępnymi w ramach osobnej płatnej subskrypcji / licencji). Oferowane narzędzie będzie oficjalnym edytorem polecanym przez producenta.**

**Uwaga: Zamawiający nie przywiązuje konkretnej wagi do nazewnictwa AV, AS, IPS pod warunkiem, że Wykonawca jest w stanie logicznie oddzielić te kategorie w taki sposób by umożliwić przejrzyste raportowanie per dana kategoria i umożliwić budowanie skutecznych polityk i reguł bezpieczeństwa. Ideą zamawiającego nie jest wskazanie konkretnych produktów tylko przyjęcie konkretnych powszechnych taksonomi.**

**Pytanie 17**

SIWZ Część 1 – punkt „System zabezpieczeń firewall musi posiadać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 600 Mbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym;

**Pytanie**: Czy przesyłanie zagrożeń do środowiska „Sand-Box” ma być wykonywane od momentu wdrożenia proponowanego rozwiązania, czy ma być opcjonalną możliwością po wykupieniu dodatkowego urządzenia/usługi?

**Odp. Przesyłanie zagrożeń do środowiska „Sand-Box” ma być wykonywane od momentu wdrożenia oferowanego rozwiązania.**

**Pytanie 18**

Dotyczy: Część 2 - System ochrony stacji końcowych użytkowników oraz serwerów

SIWZ – część 2 – „Oprogramowanie będzie zainstalowane na stacjach końcowych oraz serwerach Zamawiającego w ilości sztuk 200 w tym:

* stacje robocze
* serwery MS Windows
* serwery Linux

Oprogramowanie musi współegzystować z istniejącymi u Zamawiającego rozwiązaniami zabezpieczeń stacji końcowych typu oprogramowanie antywirusowe w zakresie ochrony przed atakami aplikacyjnymi oraz złośliwymi kodami wykonywalnymi.”

**Pytanie** 1: Czy zamawiający dopuszcza system który nie wspiera systemu Linux?

**Pytanie** 2: Koegzystowanie dwóch systemów antywirusowych (aktualny klienta oraz proponowany w zapytaniu) jest niezalecane według najlepszych praktyk. Może powodować niestabilność systemu oraz duże zużycie ilości jego zasobów. Czy zamawiający dopuszcza usunięcie z zapisów SIWZ dotyczącego konieczności współegzystencji?

**Odp 1. Zamawiający nie dopuszcza rozwiązania, które nie wspiera systemu Linux.**

**Odp. 2. Zamawiający nie dopuszcza usunięcia takiego zapisu. (por. np.: https://blog.malwarebytes.com/101/2015/09/whats-the-difference-between-antivirus-and-anti-malware/ - niniejsze porównanie nie jest wskazaniem konkretnego rozwiązania).**

**Pytanie 19**

SIWZ – część 2 – „Oprogramowanie musi posiadać agentów na systemy MS Windows oraz Linux które mogą być automatycznie generowane poprzez konsolę zarządzającą.”

Pytanie: Czy zamawiający dopuszcza system który nie wspiera systemu Linux?

Uzasadnienie: Zastosowanie zmiany będzie miało wpływ na większą liczbę oferentów oraz korzystnie wpłynie na obniżenie ceny zakupu.

**Odp. Zamawiający nie dopuszcza rozwiązania, które nie wspiera systemu Linux.**

**Pytanie 20**

SIWZ – część 2 - „Oprogramowanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela, tj. zajętość procesora nie może wynosić więcej niż 5% a zajętość pamięci RAM nie więcej niż 150MB. Dopuszcza się możliwość konfiguracji tych parametrów przez pryzmat centralnego interfejsu zarządzającego np. dla pojedynczych komputerów lub wybranych grup (np. w ramach danej polityki)”

**Pytanie**: Prosimy o zrezygnowanie wprowadzania wartości granicznych obciążeń procesora lub podania modeli procesorów używanych przez zamawiającego.

**Uzasadnienie**: Istnieje wiele generacji procesorów, których wydajność będzie znacząco różna. Wykonawca nie jest w stanie określić jakie obciążenie będzie u zamawiającego bez szczegółowych danych.

**Odp. Oprogramowanie nie może znacząco obciążać systemu, w związku z czym Zamawiający nie zrezygnuje z powyższego zapisu.**

**MODYFIKACJA TREŚCI SIWZ**

#  Działając na podstawie art. 38 ust. 4 ustawy Prawo zamówień publicznych (tj. Dz. U. z 2018 r. poz. 1986) w związku z art. 12a ustawy PZP Zamawiający dokonuje modyfikacji treści siwz w następującym zakresie:

# pkt 9 SIWZ - wykaz oświadczeń lub dokumentów składanych przez wykonawcę w postępowaniu na wezwanie Zamawiającego w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 pkt 2 ustawy PZP - Zamawiający dodaje pkt. 9.1.3. w brzmieniu:

 *9.1.3. Opis techniczny oferowanego urządzenia/oprogramowania wraz ze wskazaniem wszystkich parametrów technicznych, spełniających wymagania Zamawiającego określonych Rozdziale 4 SIWZ – zgodnie z załącznikiem nr 6 do SIWZ – dotyczy części 1 i 2.*

* Rozdział 4 – opis przedmiotu zamówienia część 1 zgodnie z udzieloną odpowiedzią do pytania 8 tj.

*„System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download”;*

* *Zamawiający dodaje załącznik nr 6 do SIWZ – Szczegółowy opis przedmiotu zamówienia*

 Jednocześnie działając na podstawie art. 38 ust. 6 ustawy Prawo zamówień publicznych (tj. Dz. U. z 2018 r. poz. 1986) Zamawiający dokonuje modyfikacji treści siwz w zakresie **przesunięcia terminu składania i otwarcia ofert na dzień 04.12.2018 r.**

SIWZ w pkt. 10.17, 14.1 i 14.2. przyjmuje następujące brzmienie :

**10.17 Ofertę wraz z oświadczeniami i dokumentami należy umieścić w zamkniętym opakowaniu, uniemożliwiającym odczytanie jego zawartości bez uszkodzenia tego opakowania. Opakowanie powinno być oznaczone nazwą (firmą) i adresem Wykonawcy, zaadresowane następująco:**

**Uniwersytet Kazimierza Wielkiego w Bydgoszczy**

**Adres: 85-064 Bydgoszcz,**

**ul. Chodkiewicza 30**

***NAZWA I ADRES WYKONAWCY***

oraz opisane:

**Numer sprawy: UKW/DZP-281-D-77/2018**

|  |
| --- |
| **„Dostawa urządzenia bezpieczeństwa sieciowego – typu next generation firewall oraz oprogramowania zabezpieczającego stacje końcowe”** |
|

**Nie otwierać przed dniem 04.12.2018 r., godz. 12:00**

1. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT
	1. Oferty powinny być złożone za pośrednictwem operatora pocztowego, kuriera lub doręczone osobiście w siedzibie Zamawiającego:

**Uniwersytet Kazimierza Wielkiego w Bydgoszczy**

**Adres: 85-064 Bydgoszcz,**

**ul. Chodkiewicza 30**

Kancelaria Główna, pokój 108, blok „C” w terminie do dnia **04.12.2018 r. do godziny 11:00**

* 1. Otwarcie ofert nastąpi wsiedzibie Zamawiającego:

**Uniwersytet Kazimierza Wielkiego w Bydgoszczy**

**Adres: 85-064 Bydgoszcz,**

**ul. Chodkiewicza 30**

pokój 61,blok „B”, w dniu **04.12.2018 r. o godzinie 12:00**

Zmodyfikowana SIWZ stanowi załącznik do niniejszego pisma.

Kanclerz UKW

mgr Renata Malak