Projekt dofinansowany z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Warmia-Mazury 2014-2020

Elbląg, dnia 30 kwietnia 2018r.

GN.272.1.1.2018.DM

TREŚĆ ZAPYTAŃ SKIEROWANCH DO ZAMAWIAJĄCEGO I WYJAŚNIENIA TREŚCI SIWZ udzielone w dniu 30 kwietnia 2018r.

Dot. postępowania GN.272.1.1.2018.DM:
Wykonanie e-usług publicznych w ramach projektu
„Projekt zintegrowanej informacji geodezyjno-kartograficznej powiatu elbląskiego"

Zamawiający informuje, że do przedmiotowego postępowania wpłynęły zapytania. Na podstawie art. 38 ustawy Prawo zamówień publicznych Zamawiający udziela wyjaśnień o następującej treści i informuje o tym wszystkich zainteresowanych.

Treść pytań oraz treść udzielanych wyjaśnień brzmi następująco:

PYTANIE 1
Czy w przypadku sprzętu komputerowego stanowiskowego (dot. 2 szt.), Zamawiający dopuści zastosowanie procesora nowszej generacji? Wymóg wydajnościowy 11 300 spełnia m.in. procesor E5-2620v4. W celu zachowania konkurencyjności postępowania prosimy o umożliwienie nam złożenia oferty na procesorze równoważnym. Chcielibyśmy zaoferować procesor, którego wyniki Dual CPU (przekraczają 15000 pkt.) publikowane są na https://www.cpubenchmark.net/cpu_lookup.php, a nie są jeszcze podawane dla PassMark CPU Mark.

Jednocześnie zwracamy się z prośbą o dopuszczenie komputera stanowiskowego wyposażonego w kartę graficzną o wydajności min. 13 400 pkt. Wydajność wręcz identyczna z wymaganą (nie ma żadnego znaczenia dla faktycznej wydajności), ale umożliwia zaproponowanie konfiguracji komputera spełniające wszystkie pozostałe wymagania łącznie.

ODPOWIEDŹ 1
Zamawiający informuje, że dokonał Zmiany treści SIWZ Nr 1, w której dokonał zmiany zapisów OPISU PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ II stanowiącego ZAŁĄCZNIK NR 12 do SIWZ.
Zamawiający dopuszcza zastosowanie procesora nowszej generacji. Zamawiający dopuści zastosowanie komputera wyposażonego w kartę graficzną o wydajności min. 13 400 pkt. Zamawiający wprowadził odpowiednie zmiany do załącznika nr 12 do SIWZ.

PYTANIE 2
Czy Zamawiający dopuści komputer (laptop), który będzie wyposażony w procesor o wydajności 9450 pkt. wg https://www.cpubenchmark.net/cpu_list.phpna dzień 15.04.2018.

ODPOWIEDŹ 2
Zamawiający informuje, że dokonał Zmiany treści SIWZ Nr 1, w której dokonał zmiany zapisów OPISU PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ II stanowiącego ZAŁĄCZNIK NR 12 do SIWZ.
Zamawiający dopuszcza zastosowanie procesora wydajności min. 9450 pkt. osiągający wynik z dnia 15.04.2018 r. Zamawiający wprowadził odpowiednie zmiany do załącznika nr 12 SIWZ.

PYTANIE 3

Zwracamy się do Zamawiającego z wnioskiem do dopuszczenie rozwiązania stanowiącego alternatywę sprzętową dla rozwiązania, które bardzo szczelnie zostało opisane poprzez liczny zbiór wymagań wydajnościowo-funkcjonalnych spełnianych przez tylko jednego producenta – firmę Fortinet z systemem Fortigate 900D/1000D.

W związku z jawnym ograniczeniem konkurencyjności, wnioskujemy do Państwa o odstąpienie od niektórych wymagań spełnianych wyłącznie przez Fortinet, lub zastąpienie ich parametrami czy funkcjonalnościami zbieżnymi do opisanymi (np. funkcjonalnościami podobnymi ale realizowanymi w alternatywny sposób). Bez uszczerbku dla funkcjonalności bezpieczeństwa e-usług, dla których zamierzcie wdrożyć system bezpiecznych połączeń.

a) Wymóg: System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

Pytanie: Prosimy o odstąpienie od zapisu "monitorowania na porcie SPAN". Funkcje SPAN realizowane jest z reguły na urządzeniach aktywnych sieci, tj. switchach i nie ma potrzeby by była aktywowana na brzegu sieci.

b) Wymóg: W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.

Pytanie: Prosimy o odstąpienie od tej części wymogu, która mówi o możliwości budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów.

Możliwość tworzenia tzw. VDOMów wg nomenklatury Fortinet jest funkcjonalnością charakterystyczna tylko dla nich. W Państwa projekcie nie ma takiej potrzeby, a tak postawiony wymóg ogranicza konkurencyjność postępowania.

c) Wymóg: W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

Pytanie: prosimy o odstąpienie od wymogu budowy rozwiązania w trybie klastra Active-Active.

Ten wymóg spełniają wyłącznie urządzenia Fortinet. Wydajne, bezpieczne, a dodatkowo efektywne środowisko można zbudować w trybie Active-Passive. W Państwa przypadku, co zresztą potwierdzają wymagania wydajnościowe, środowisko w trybie Active-Passive spełni swoją rolę z dużym zapasem.

Wymagania wydajnościowe:
Zwracamy się do Zamawiającego o dopuszczenie rozwiązania, dla którego:
- w zakresie Firewall będzie możliwa obsługa nie mniej niż 10 mln jednoczesnych połączeń oraz 180.000 nowych połączeń na sekundę.
- przepustowość Stateful Firewall będzie nie mniejsza niż 25 Gbps w trybie dla ruchu IMIX oraz nie mniejsza niż 30 Gbps dla ruchu pakietów, których rozmiar ustalają laboratoria certyfikujące.
- przepustowość Firewall z włączoną funkcją Kontroli Aplikacji będzie nie mniejsza niż 10 Gbps.
- wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256 będzie nie mniejsza niż 10 Gbps.
- Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 4 Gbps.
- Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.

Prosilibyśmy o odstąpienie od wymogu brzmiącego Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 4 Gbps.
Dla funkcji bezpieczeństwa prosilibyśmy o wprowadzenie następujących zmian.
- Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS

- Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3 tj. odstąpienie od protokołu IMAP w obu przypadkach.

Protokół IMAP działa bezpośrednio na serwerze pocztowym. Wszelkie zagrożenia Wirus powinien zanim zainfekują serwer są wyłapywane na protokole SMTP.

Prosilibyśmy o odstąpienie od następujących zapisów.

- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
- Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

Dla funkcji routingu i obsługi WANu.

- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.

Prosimy o odstąpienie od wymogu dla protokołu PIM, który to jest charakterystyczny chociażby dla operatorów multimedialnych wykorzystujący go w realizacji multikastów. U Państwa takiej potrzeby nie będzie. Zapis postawiony pierwotnie w SIWZ jest charakterystyczny dla firmy Fortinet.

Dla funkcji ochrony przed atakami

Prosimy o odstąpienie od zapisu: „Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora" i zamianę tego wymogu na:

„Baza sygnatur ataków powinna zawierać min.1500 wpisów"

Certyfikaty

Prosimy o wprowadzenie zapisu umożliwiającego zaoferowanie urządzeń posiadających certyfikaty równoważne, obowiązujące na terenie EU.

Prosilibyśmy o zastąpienie wymogu posiadania certyfikatów (charakterystycznych dla produktów kierowanych na rynek amerykański)

· ICSA lub EAL4 dla funkcji Firewall
· ICSA lub NSS Labs dla funkcji IPS
· ICSA dla funkcji: SSL VPN, IPSec VPN

Na następujące certyfikaty.

· ICSA lub EAL4 dla oferowanego urządzenia
· Certyfikat ICSA lub rekomendacja respektowana przez NATO i Unię Europejską NATO Restricted i UE Restricted.

Poprzez aktualnie postawiony wymóg SIWZ uniemożliwiacie Państwo zaoferowanie systemów bezpieczeństwa producentom, który certyfikowali swoje urządzenia wedle alternatywnych, równoważnych wymagań obowiązujących w Unii Europejskiej.

ODPOWIEDŹ 3

Zamawiający informuje, że dokonał Zmiany treści SIWZ Nr 1, w której dokonał zmiany zapisów OPISU PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ II stanowiącego ZAŁĄCZNIK NR 12 do SIWZ.

Zamawiający uznał w całości zastrzeżenia oraz zmienił zapisy załącznika nr 12 do SIWZ w powyższym zakresie.

PYTANIE 4

Serwery

a) Prosimy o określenie minimalnej wydajności procesora w SPEC w teście CINT2006 Rates, opublikowanej przez SPEC.org (www.spec.org). W specyfikacji brakuje wyniku SPEC.

b) Karty sieciowe zamawiający podaje - min. 2 karty FC 16Gbps

Prosimy o doprecyzowanie: Jakie mają to być karty FC? Single/Dual port? Proszę pamiętać, że udzielając odpowiedzi należy to powiązać z macierzą.

c) Zamawiający podaje dla Systemu operacyjnego: Microsoft Windows Server, 25 x windows Serwer CAL

W jakiej edycji wykonawca miałby dostarczyć system operacyjny? Jakie CAL do serwera - Użytkownik/Urządzenie?

ODPOWIEDŹ 4

Zamawiający informuje, że dokonał Zmiany treści SIWZ Nr 1, w której dokonał zmiany zapisów OPISU PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ II stanowiącego ZAŁĄCZNIK NR 12 do SIWZ.

Zamawiający uznał w całości zastrzeżenia oraz zmienił zapisy załącznika nr 12 do SIWZ w powyższym zakresie.

PYTANIE 5
Macierz pamięci masowej.
Jaka replikacja w macierzy? Zakładamy, że jest to replikacja synchroniczna, powszechna w projektach o podobnych oddziaływaniu i przygotowaniu infrastruktury pod e-usługi.
Co Zamawiający definiuje pod pojęciem „replikacja on-line"?
Jaką gwarancją należy objąć macierze?
Co Zamawiający chce zrealizować? W jakiej konfiguracji mają pracować urządzenia? Czy ma być jakiś klaster? (bez switcha FC to będzie to działać poprawnie). Prosimy o przedstawienia planowanej architektury.

ODPOWIEDŹ 5
Zamawiający informuje, że dokonał Zmiany treści SIWZ Nr 1, w której dokonał zmiany zapisów OPISU PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ II stanowiącego ZAŁĄCZNIK NR 12 do SIWZ.
Zamawiający zmienił zapisy załącznika nr 12 do SIWZ w powyższym zakresie.
Jednocześnie zamawiający informuje, że okres gwarancji liczony jest dla całego zaoferowanego sprzętu zgodnie z okresem zaoferowanym przez Wykonawcę (jest to kryterium punktowe). Okres gwarancji udzielanej przez Wykonawcę nie może być krótszy niż 24 miesiące. Wykonawca zamówienia, który zaproponuje minimalny okres gwarancji, tj. 24 miesiące otrzyma 0 pkt. Wykonawca zamówienia, który zaproponuje maksymalny okres gwarancji, tj. 60 miesięcy otrzyma 100 pkt.

PYTANIE 6
W ramach opisu wyposażenia serwerowni Zamawiający wymienia 2 serwery + macierz dyskową. Czy wymienione urządzenia mają pracować w klastrze? Jeżeli tak, jakiego typu klaster Zamawiający ma na uwadze?

ODPOWIEDŹ 6
Przewidywany klaster typu active-active.

PYTANIE 7
W opisie serwerów Zamawiający specyfikuje procesor, jednak nie określa w sposób jednoznaczny wymogów wydajnościowych w postaci wyników SpecIntRate – zwracamy się z prośbą o doprecyzowanie wymogów wydajnościowych.

ODPOWIEDŹ 7
Zamawiający informuje, że dokonał Zmiany treści SIWZ Nr 1, w której dokonał zmiany zapisów OPISU PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ II stanowiącego ZAŁĄCZNIK NR 12 do SIWZ.
Zamawiający wprowadził odpowiednie zmiany do załącznika nr 12 do SIWZ.

PYTANIE 8
W opisie serwerów Zamawiający specyfikuje dyski twarde jako 6x600GB pracujące w trybie RAID1. Mając na uwadze fakt, iż przedmiotem zamówienia są również macierze zwracamy się z prośbą o wyjaśnienie, czym podyktowana jest aż tak duża pojemność dyskowa serwerów oraz tryb RAID1, który w tej sytuacji zgodnie z dobrą praktyką projektowania architektur DC wydaje się być wymogiem bezzasadnym.

ODPOWIEDŹ 8
Konfiguracja sprzętu wynika z założeń projektowych, na które Zamawiający uzyskał dofinansowanie.

PYTANIE 9
W opisie serwerów Zamawiający specyfikuje moc zasilaczy na poziomie 1100W, mając na uwadze wyspecyfikowane komponenty warto zauważyć, iż przedmiotowa moc zasilacza jest wymogiem na wyrost, prosimy o wyjaśnienie czym podyktowany jest tak wysoki parametr mocy dla zasilaczy serwerowych.

ODPOWIEDŹ 9
Konfiguracja sprzętu wynika z założeń projektowych, na które Zamawiający uzyskał dofinansowanie.

PYTANIE 10
W opisie serwerów Zamawiający specyfikuje karty FC – prosimy o wyjaśnienie, ilu portowe mają to być karty?

ODPOWIEDŹ 10
Zamawiający informuje, że dokonał Zmiany treści SIWZ Nr 1, w której dokonał zmiany zapisów OPISU PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ II stanowiącego ZAŁĄCZNIK NR 12 do SIWZ.
Zamawiający wprowadził odpowiednie zmiany do załącznika nr 12 do SIWZ.

PYTANIE 11
W opisie serwerów Zamawiający specyfikuje system operacyjny MS Windows Server, prosimy o informację jakiego rodzaju Windows Server ma zostać dostarczony, jednocześnie prosimy o określenie jakiego rodzaju licencje dostępowe CAL, per Device czy per User, mają zostać dostarczone w ramach zamówienia.

ODPOWIEDŹ 11
Zamawiający informuje, że dokonał Zmiany treści SIWZ Nr 1, w której dokonał zmiany zapisów OPISU PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ II stanowiącego ZAŁĄCZNIK NR 12 do SIWZ.
Zamawiający wprowadził odpowiednie zmiany do załącznika nr 12 do SIWZ.

PYTANIE 12
W opisie Macierzy pamięci masowej Zamawiający specyfikuje jak poniżej:
„Komplet 2 szt. współpracujących ze sobą macierzy dyskowych typu Fibre Channel w obudowach maksymalnie 2U każda."
a) Jakiego klastra oczekuje Zamawiający? Zautomatyzowanego tzw Disaster Recovery? Czy też zwyczajnej repliki danych na drugiej macierzy?
b) Czy Zamawiający dysponuje przełącznikami FC pozwalającymi na spięcie rzeczonych macierzy w klaster?
c) Zamawiający specyfikuje co następuje „obsługa w trybie bezpośrednim minimum 7 serwerów" , w kontekście pozostałych parametrów macierzy wymóg ten wydaje się być mocno zawyżony. Pozostałe parametry wskazują na macierz typu entry, tymczasem obsługa 7 urządzeń w trybie point-to-point charakterystyczna jest dla macierzy typu High end. Ponadto nie jest to konfiguracja zalecana przez producentów przez wzgląd na brak wykorzystania podstawowych mechanizmów macierzowych. Zwracamy się zatem z zapytaniem, czy Zamawiający zrezygnuje z przedmiotowego zapisu?

ODPOWIEDŹ 12
Zamawiający oczekuje klastra Disaster Recivery. Przewidywany klaster typu active-active.
Zamawiający nie posiada przełącznika, dostawca powinien uwzględnić przełącznik jako element wymagany dla uruchomienia systemu.

PYTANIE 13
A) Dotyczy: System bezpiecznego połączenia
W związku z opisem przedmiotu zamówienia części II „Dostawa sprzętu teleinformatycznego w ramach projektu pn. „Projekt zintegrowanej informacji geodezyjno-kartograficznej powiatu elbląskiego" System służący do utworzenia bezpiecznego połączenia pozwalamy sobie zwrócić Państwa uwagę na następujące kwestie:
Zgodnie z dyspozycją art. 29 ustawy PZP przedmiot zamówienia winien być opisany w sposób neutralny. Zamawiający nie może opisywać przedmiotu zamówienia ani stawiać warunków udziału w postepowaniu w taki sposób, aby utrudniać uczciwą konkurencję, dostęp do zamówienia publicznego innym wykonawcom oferującym rozwiązania równoważne ani uzależniać wyniku postępowania od trzeciej strony, a tak jest w niniejszym przypadku.
Pragniemy zwrócić Zamawiającemu uwagę na kilka istotnych zapisów uniemożliwiających złożenie oferty na systemie równoważnym. Aktualne zapisy stanowią takie ukompletowanie wymagań, że tylko jeden producent spełnia je łącznie.
I. „Redundancja, monitoring i wykrywanie awarii
...

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN."
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.
II. Redundancja, monitoring i wykrywanie awarii
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
III. Parametry wydajnościowe:
W zakresie Firewall'a obsługa nie mniej niż 11 mln jednoczesnych połączeń oraz 280.000 nowych połączeń na sekundę.
Przepustowość Stateful Firewall: nie mniej niż 25 Gbps dla pakietów 512 B.
Przepustowość Stateful Firewall: nie mniej niż 30 Gbps dla pakietów 64 B.
Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 10 Gbps.
Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 25 Gbps.
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 4 Gbps.
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 4 Gbps.
IV. Funkcje Systemu Bezpieczeństwa:
4.Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
…
7.Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
…
9.Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10.Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
…
V. Routing i obsługa łączy WAN
…
Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM
…
VI. Ochrona przed atakami
…
Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
VII. Certyfikaty
Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
ICSA lub EAL4 dla funkcji Firewall
ICSA lub NSS Labs dla funkcji IPS
ICSA dla funkcji: SSL VPN, IPSec VPN
….."

Postulat zapewnienia uczciwej konkurencji oznacza konieczność eliminacji z opisu przedmiotu zamówienia wszelkich sformułowań, które wykluczałyby wykonawców, uniemożliwiając im złożenie oferty na rozwiązaniach podobnych lub powodując sytuację, w której jeden z zainteresowanych wykonawców byłby bardziej uprzywilejowany od pozostałych.

Ad. I. oraz II. Redundancja, monitoring i wykrywanie awarii
Większość dostępnych na rynku rozwiązań firewall daje możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT i transparentnym. Funkcje SPAN portu są realizowane poprzez przełączniki sieciowe i w nie jest to funkcja używana w urządzeniach brzegowych, ponieważ te urządzenia mają własną kontrolę IPS

same w sobie, nie muszą wysyłać transmisji do kolejnego urządzenia kontrolującego ruch sieciowy. Tym bardziej, że takie urządzenie nie jest przedmiotem bieżącego postępowania. SPAN port jest to cechą charakterystyczna dla urządzenia Fortigate firmy Fortinet.

Większość rozwiązań na rynku obsługuje jedną instancję, zaś w ramach tej instancji jest możliwość konfigurowania Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Ponadto istnieje możliwość równoczesnego ustawienia w tym samym czasie dwóch trybów: Routera z funkcją NAT i transparentnym przez co więcej niż jedna instancja nie jest potrzebna. Jeżeli jest możliwość dedykowania co najmniej 8 administratorów systemu to nie ma w niniejszym wykorzystaniu firewalla uruchamiać więcej niż jednej instancji. Wiele instancji (tj. do 10 w ramach podstawowej licencji) jest cechą charakterystyczna dla urządzenia Fortigate firmy Fortinet.

Tryb HA Active-Passive cechuje się atrakcyjnością cenową łącząc dwa urządzenia w trybie niezawodnościowy. Skalując rozwiązanie docelowo już na etapie projektowania można przewidzieć zwiększenie mocy głównego urządzenia niż sztuczne zwiększanie jej za pomocą łączenia i wykorzystania mocy drugiego urządzenia. W konfiguracji Active-Active z góry będziemy skazani na włączenie tylko części swojej mocy zapasowego urządzenia, ponieważ będzie mu przydzielać do realizacji główne urządzenie. Zatem wzrost mocy poprzez taki klaster nie będzie specjalnie zauważalny, w porównaniu z tym gdy od razu zaplanujemy większą moc na urządzeń w klastrze niezawodnościowym Active-Passive. Klaster Active-Active jest cechą charakterystyczna dla urządzenia Fortigate firmy Fortinet.
Ad. III Parametry wydajnościowe
Parametry wydajnościowe wskazują platformę FG-1000D firmy Fortinet. Żaden inny producent nie jest w stanie spełnić wszystkich wymagań łącznie. Poniżej przedstawiamy parametry wydajnościowe, które z bardzo dużą nawiązką zapewnią wydajną i bezpieczną sieć połączeń użytkowników e-usług.
Ad. IV Funkcje Systemu Bezpieczeństwa
Prosimy o usunięcie zapisów dotyczącego ochrony przed wirusami dla protokołu IMAP. Protokół IMAP działa bezpośrednio na wiadomościach na serwerze pocztowym. Wirus powinien być wyłapany zanim trafi na serwer poprzez ochronę przed wirusami na protokole SMTP. Za pomocą protokołu IMAP użytkownik pobiera tylko nagłówki wiadomości, sama wiadomość i załączniki są pobierane na żądanie użytkownika. Wiadomości zostają są serwerze. Jest to cecha charakterystyczna dla urządzenia Fortigate firmy Fortinet.
System DLP na urządzeniu brzegowym musi rozpoznawać rodzaj dokumentu, z rozróżnieniem różnych wersji aplikacji, wyszukać ciąg znaków, które mają być zablokowane w zależności od rodzaju dokumentu. Mechanizm ten bardzo obciąża urządzenie brzegowe, i nie jest bardzo skuteczny, więc sugeruje się umieszczenie tego mechanizmu na urządzeniach roboczych użytkowników. Idea ta jest realizowana przez aplikacje typu DLP na komputerze, które bardziej skutecznie realizują to wymaganie (np. oprócz zapobieganiu wycieku danych poprzez pocztę czy stronę Internetową również zapobiegnie wyciekowi poprzez zasoby sieciowe, zewnętrzny nośnik pamięci jak USB czy płyta CD) i nie obciąży urządzenia brzegowego przed realizacją zadań i analizy transmisji. Prosimy o usunięcie zapisów dotyczącego mechanizmu ochrony przed wyciekiem poufnej informacji (DLP) ponieważ wielu producentów rozumie, że jest to mechanizm który powinien być konfigurowany na stacjach roboczych a nie na firewallu. DLP jest tylko cechą charakterystyczna dla urządzenia Fortigate firmy Fortinet.

Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych również jest cechą charakterystyczną dla urządzenia Fortigate firmy Fortinet. Fortinet dostarcza 2 tokeny sprzętowe lub programowe, które mogą być zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Pozostałe urządzenia dostępne na rynku realizują to zadanie poprzez pojedyncze uwierzytelnianie bez tokenów sprzętowych. Zgodnie z zasadą konkurencji istnieje możliwość skorzystania z tokenów sprzętowych firm trzecich, jednakże dwuskładnikowe uwierzytelnianie jest to elementem niniejszego postepowania. Zatem prosimy o usunięcie zapisów dotyczącego dwu-składnikowego uwierzytelniania z wykorzystaniem tokenów sprzętowych lub programowych oraz dostarczenia co najmniej 2 tokeny sprzętowe lub programowych, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
Ad. V Routing i obsługa łączy WAN
W niniejszym postępowaniu chodzi o to aby dostarczyć urządzenie do ochrony sieci a nie router multikastów do obsługi cyfrowej telewizji Internetowej, którą realizują dostawcy usług Video on Demand. Statycznym routingu multikastów w zupełności powinien być wystarczający na urządzeniu brzegowym. Prosimy o usunięcie zapisu dotyczącego dynamicznego protokołu PIM. Prosimy o zmianę zapisu na następujący: „Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP. PIM jest cechą charakterystyczna dla urządzenia Fortigate firmy Fortinet.

Ad. VI Ochrona przed atakami
Czy Zamawiający pozwoli na urządzenie, którego system IPS pozwoli w sposób szybszy niż przedstawiony w wymaganiu zrealizowanie analizy bezpośrednio w jądrze systemu? Analiza protokołu może być kontrolowana tak, że dla poszczególnych typów ruchu sieciowego w warstwie aplikacji opracowane zostały specjalne wtyczki programowe (tzw. pluginy), pracujące w trybie kernel-mode, czyli bezpośrednio w jądrze systemu operacyjnego. Po wykryciu określonego typu ruchu (np. HTTP, FTP, SMTP, ...) automatycznie uruchamiana jest odpowiednia wtyczka, która specjalizuje się w ochronie danego protokołu. Rodzaj stosowanych zabezpieczeń dynamicznie dostosowywany jest do rodzaju przepływającego ruchu. Następnie jest rozpoznawany typowy ciągów danych. W tym przypadku zasadnicze znaczenie ma kontekst, w jakim zostały wykryte pakiety charakterystyczne dla określonego ataku. Kontekstem są tutaj np. rodzaj połączenia, protokół czy port. W ten sposób sieć jest chroniona przed najnowszymi zagrożeniami, dla których sygnatury jeszcze nie powstały. Dzięki temu mechanizmowi można wykryć ponad 10 000 różnych zagrożeń, zaś wystarczy na to tylko około 1500 wpisów.
Ilość 5 000 wpisów opisanych w sposób jak w SIWZ, to cecha charakterystyczna dla urządzenia Fortigate firmy Fortinet.
Ad. VII Certyfikaty
Prosimy o zmianę wymagania dotyczącego posiadania certyfikacji ICSA Labs i NSS Labs na wymóg posiadania certyfikatów wystawianych i respektowanych przez NATO i Unię Europejską m.in. NATO Restricted czy EU Restricted. Firma certyfikująca ICSA Labs znajduje się w Stanach Zjednoczonych i certyfikuje urządzenia, które są oferowane do amerykańskiego rynku odbiorców systemów bezpieczeństwa. Wymaganie to dyskwalifikuje producentów europejskich, którzy przede wszystkim oferują swoje rozwiązania do odbiorców systemów bezpieczeństwa na rynku europejskim. Zamawiający reprezentuje Polską instytucję zarówno w kraju, jak i w Unii Europejskiej, powinien raczej wymagać certyfikacji i raportów, które nadawane są w Europie jak np. NATO Restricted czy EU Restricted, które są równoważne do certyfikatu ICSA .
Certyfikacja NATO jest oficjalną rekomendacją rozwiązań związanych z ochroną i bezpieczeństwem informacji dla państw członkowskich NATO.
Wnosimy w związku z powyższym, w celu zapewnienia przestrzegania zasad uczciwej konkurencji i równego dostępu do zamówienia, o stosowną modyfikację opisu poprzez:
I. Redundancja, monitoring i wykrywanie awarii
Jest:
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
Proponowana zmiana:
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT i transparentnym.
Jest:
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.
Proponowana zmiana:
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy systemu w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów systemu.
II. Redundancja, monitoring i wykrywanie awarii
Jest:
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
Proponowana zmiana:
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Passive. Dopuszcza się również możliwość łączenia w klaster Active-Passive ale nie jest wymagana. Powinna istnieć funkcja synchronizacji sesji firewall.
III. Parametry wydajnościowe:
Jest:
W zakresie Firewall'a obsługa nie mniej niż 11 mln jednoczesnych połączeń oraz 280.000 nowych połączeń na sekundę.
Przepustowość Stateful Firewall: nie mniej niż 25 Gbps dla pakietów 512 B.
Przepustowość Stateful Firewall: nie mniej niż 30 Gbps dla pakietów 64 B.

Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 10 Gbps.
Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 25 Gbps.
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 4 Gbps.
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 4 Gbps.
Proponowana zmiana:
W zakresie Firewall'a obsługa nie mniej niż 9 mln jednoczesnych połączeń oraz 170.000 nowych połączeń na sekundę.
Przepustowość Stateful Firewall: nie mniej niż 24 Gbps dla ruchu IMIX.
Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów generowanych przez laboratoria badające wydajność.
Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 8 Gbps.
Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 10 Gbps.
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP – min. 4 Gbps.
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – min. 3 Gbps.
Prosimy o wykreślenie punktu 8:
Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 4 Gbps.
IV. Funkcje Systemu Bezpieczeństwa:
Jest:
4.Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
7.Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
...
9.Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10.Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
Proponowana zmiana:
4.Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS.
...
7.Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
...
Prosimy o wykreślenie punktów 9 i 10:
9.Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10.Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
...
Dla Pastwa potrzeb system bezpieczeństwa o przedstawionych nowych wymaganiach wydajnościowych będzie w zupełności wystarczający, gwarantując dodatkowo bardzo dużą rezerwę na przyszłość. Systemy o takiej wydajności są implementowane w bardzo dużych ośrodkach miejskich.
V. Routing i obsługa łączy WAN
Jest:
Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM
Proponowana zmiana:
Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.
VI. Ochrona przed atakami
Jest:
Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

Proponowana zmiana:
2.Baza sygnatur ataków powinna zawierać minimum 1500 wpisów
VII. Certyfikaty
Jest:
Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
ICSA lub EAL4 dla funkcji Firewall
ICSA lub NSS Labs dla funkcji IPS
ICSA dla funkcji: SSL VPN, IPSec VPN
Proponowana zmiana:
ICSA lub EAL4 dla oferowanego urządzenia
Certyfikat ICSA lub rekomendacja respektowana przez NATO i Unię Europejską NATO Restricted i UE Restricted.
B) Dotyczy Sprzęt komputerowy stanowiskowy - 2 szt.
Pytanie 1.
Zamawiający podaje w SIWZ, iż dla wydajnego sprzętu komputerowego dla stanowisk GIS oczekuje konfiguracji wyposażonej w - 2 x Procesor: Osiągający w teście PassMark CPU Mark wynik min. 11300 punktów według wyników ze strony https://www.cpubenchmark.net/cpu_list.php z dnia 22-03-2018r.
W przypadku wydajnych stacji roboczych, producenci sprzętu komputerowego, dynamicznie wprowadzają do swojej oferty nowe procesory. Cykl życia samych procesorów, podobnie jak kompletnych stacji roboczych, jest krótki i nieprzewidywalny w kontekście wprowadzenia nowości. Zmiany ewoluują w krótkich odstępach czasu i bazujące na co rusz innych komponentach. Procesory są jednym z głównie ewoluujących komponentów sprzętu komputerowego. Zdarza się, że dla procesorów nowszej generacji nie jest jeszcze publikowany wynik na https://www.cpubenchmark.net/cpu_list.php jako PassMark CPU Mark, tylko wynik Dual CPU dostępny także na https://www.cpubenchmark.net/cpu_lookup.php
Procesorem, którego wynik na PassMark w dniu 22.03.2018 r przekraczał wymagane w SIWZ 11300 pkt., był procesor Intel E5-2630v4@2,2GHz, który przez licznych producentów komputerów został zastąpiony innym. Dla podanego procesora aktualna wartość CPU Mark wynosi aktualnie 13 903 pkt (prezentuje to zrzut ekranu na dn. 24.04.2018 z https://www.cpubenchmark.net/cpu_list.php
Popular comparisons for Intel Xeon Silver 4108 @ 1.80GHz
As of 24th of April 2018 - Higher results represent better performance
Intel Xeon Silver 4108 @ 1.80GHz
15,441
Intel Xeon W-2135 @ 3.70GHz
16,460
Intel Xeon Silver 4114 @ 2.20GHz
14,466
Intel Xeon E5-2618L v4 @ 2.20GHz
14,592
AMD EPYC 7251 8-Core
11,833
Intel Xeon Silver 4116 @ 2.10GHz
16,723
AMD EPYC 7401P
18,465
AMD EPYC 7351P
17,991
Intel Xeon E5-1650 v3 @ 3.50GHz
13,604
Intel Xeon E5-2640 v3 @ 2.60GHz
14,077
Intel Xeon E5-2630 v4 @ 2.20GHz
13,903
Intel Xeon E5-2640 v4 @ 2.40GHz
15,331
Intel Xeon E5-2687W @ 3.10GHz
14,404
Intel Xeon E5-2667 v2 @ 3.30GHz
16,093
Intel Xeon E5-2650 v3 @ 2.30GHz

14,880
Intel Xeon Silver 4110 @ 2.10GHz
11,631
Intel Xeon W-2145 @ 3.70GHz
19,936
PassMark Software © 2008-2018
Zwracamy się do Zamawiającego z wnioskiem o dopuszczenie komputera, w którym zostaną zastosowane procesory o wydajności przekraczającej wynik 15 000 pkt. wg Dual CPU (https://www.cpubenchmark.net/cpu_lookup.php)
Pytanie 2
Zamawiający podaje w SIWZ, iż dla wydajnego sprzętu komputerowego dla stanowisk GIS oczekuje konfiguracji wyposażonej w - Karta graficzna: Oferująca odpowiednią moc do obsługi wspomaganego komputerowo projektowania, wytwarzania oraz prac inżynieryjnych, osiągająca w teście PassMark Performance Test wynik min. 13500 punktów (G3D Rating) według wyników ze strony: http://www.videocardbenchmark.net/gpu_list.php z dnia 22-03-2018r.
Kartą graficzną, która na dzień 22.03.2018 spełniała wymóg 13 500 pkt. jest karta Quadro P6000. Jej wynik na dzień dzisiejszy (tj.24.04) jest na poziomie 13 499 pkt.
Prosimy Zamawiającego o wyrażenie zgody na zastosowanie ww. karty graficznej.
C) Dotyczy Laptopy - 3 szt.
Zamawiający podaje w SIWZ, iż dla laptopów oczekuje konfiguracji wyposażonej w: - Procesor wielordzeniowy, osiągający w teście PassMark CPU Mark wynik min. 9500 punktów według wyników ze strony https://www.cpubenchmark.net/cpu_list.php z dnia 22-03-2018r.
Procesorem, który na dzień 22.03.2018 spełniał wynik 9500 pkt. był Intel Core i7-7820HQ @ 2.90GHz, którego aktualny (tj. na 24.04.2018) wynik wynosi 9461 pkt.
W przypadku procesorów tendencja jest zmienna, raz wyniki publikowane na https://www.cpubenchmark.net/cpu_list.php rosną w czasie, by w innym momencie wykazywać tendencję spadkową. Dlatego prosimy Zamawiającego o wyrażenie zgody na zastosowanie procesora Intel Core i7-7820HQ @ 2.90GHz.
D) Dotyczy Macierzy – 2 szt.
Co Zamawiający rozumie przez pojęcie „replikacja on-line"?
Prosimy Zamawiającego o podanie, o jakiej replikacji w macierzy myślał określając przedmiotowy wymóg – synchronicznej czy asynchronicznej?
Prosilibyśmy podać minimalny okres gwarancji dla macierzy oraz warunki szczegółowe jej świadczenia?
Prosilibyśmy o określenie przynajmniej ogólnych założeń dla zaplanowanej konfiguracji. Podanie w SIWZ tylko wymagań dla samych elementów bez przedstawienia założeń, do czego ma służyć, jak ma to pracować ….- często doprowadza do nieporozumień w realizacji.
E) Dotyczy Serwerów – 2 szt.
prosimy o podanie w jakiej wersji wykonawca ma dostarczyć system operacyjny dla serwerów oraz jakiego rodzaju licencje CAL powinny być uwzględnione w wycenie (device/user)

ODPOWIEDŹ 13
Zamawiający informuje, że dokonał Zmiany treści SIWZ Nr 1, w której dokonał zmiany zapisów OPISU PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ II stanowiącego ZAŁĄCZNIK NR 12 do SIWZ.
Zamawiający uznał w całości zastrzeżenia oraz zmienił zapisy załącznika nr 12 do SIWZ w powyższym zakresie.
Zamawiający oczekuje klastra Disaster Recivery. Przewidywany klaster typu active-active.
Jednocześnie zamawiający informuje, że okres gwarancji liczony jest dla całego zaoferowanego sprzętu zgodnie z okresem zaoferowanym przez Oferenta (jest to kryterium punktowe). Okres gwarancji udzielanej przez Wykonawcę nie może być krótszy niż 24 miesiące. Wykonawca zamówienia, który zaproponuje minimalny okres gwarancji, tj. 24 miesiące otrzyma 0 pkt. Wykonawca zamówienia, który zaproponuje maksymalny okres gwarancji, tj. 60 miesięcy otrzyma 100 pkt.

ZARZĄD POWIATU
w ELBLĄGU

CZŁONEK ZARZĄDU
Joanna Naszińska

WICESTAROSTA
mgr Zbigniew Lichuszewski