Wojewódzki Szpital Specjalistyczny im. Najświętszej Maryi Panny
42-200 Częstochowa, ul. Bialska 104/118
tel. i faks: (34) 367-36-74
e-mail: szp@dala.pl

Częstochowa, dnia 24 maja 2018 r.

Znak sprawy: DAZ.26**.038.2018 r.**

L. dz. 1759/2018 r.

Wszyscy zainteresowani

Dotyczy: postępowania o udzielenie zamówienia publicznego na ,,Dostawę firewalla dla Wojewódzkiego Szpitala Specjalistycznego im. Najświętszej Maryi Panny w Częstochowie wraz z wymianą firewalla, konfiguracją oraz szkoleniem pracowników".

WYJAŚNIENIA TREŚCI SIWZ - NR 1

Na podstawie art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2017 r., poz. 1579 z późn. zm.), zwanej dalej ,,ustawą", Wojewódzki Szpital Specjalistyczny im. Najświętszej Maryi Panny w Częstochowie, przedstawia treść zapytań dotyczących zapisów Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej SIWZ wraz z wyjaśnieniami.

W przedmiotowym postępowaniu przed upływem połowy wyznaczonego terminu składania ofert wpłynęły następujące pytania:

PYTANIE 1:

Dotyczy: Firewall
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. „Wymagania ogólne
Jest:
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.
Wyjaśnienie:
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.

Proponowana zmiana:
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym lub hybrydowym.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do systemu.
Odpowiedz:
Zamawiający wymaga aby dostarczony system umożliwiał pracę w różnych trybach, w tym Routera z funkcją NAT, transparentnym oraz w trybie monitorowania na porcie SPAM. Funkcja monitorowania na porcie SPAN , lub Mirro porcie jest obecna w wielu rozwiązaniach bezpieczeństwa dostępnych na rynku. Zamawiającemu nie chodzi o możliwość konfiguracji SPAN portu na systemie bezpieczeństwa ale raczej o możliwość podpięcia do tego typu portu na przełączniku. Po to aby cała komunikacja kopiowana przez przełącznik na taki port była analizowana przez system bezpieczeństwa. W ten sposób jeden z logicznych systemów może zostać skonfigurowany do pasywnego nasłuchu i analizy komunikacji sieciowej. System ten powinien być odseparowany logicznie od systemu podstawowego z możliwością przydzielenia do niego dostępu dla zdefiniowanych administratorów.
Dlatego Zamawiający podtrzymuje swoje wymagania.

PYTANIE 2:

Tabela Nr I
Punkt 4. 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.
Wyjaśnienie:
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.

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-Active ale nie jest wymagany. Powinna istnieć funkcja synchronizacji sesji firewall.
Odpowiedz:
Funkcja klastra Active Atctive jest dostarczana przez wielu producentów rozwiązań typu Next Generation Firewall. Zamawiający musi mieć na uwadze fakt, że ochrona przed ewoluującymi zagrożeniami będzie wymagała implementacji coraz bardziej wymagających funkcji ochronnych. Konfiguracja Active Avctive będzie alternatywą dla takiej sytuacji jeśli wystąpi w przyszłości dlatego zakupione rozwiązanie powinno umożliwiać pracę w klastrze Active – Active.
Nie zmienia to faktu, że w ramach postępowania elementy systemu muszą dostarczać wydajności oszacowanej na chwilę obecną, opisanej w SIWZ.
Zamawiający podtrzymuje zapisy.

PYTANIE 3:

5. Parametry sprzetowe
Jest:
18 portami Gigabit Ethernet RJ45.
16 gniazdami SFP 1 Gbps
System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB
Wyjaśnienie:
Parametry wydajnościowe wskazują platformę Fortigate FG-301E 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.
Proponowana zmiana:
10 portami Gigabit Ethernet RJ45.
16 gniazdami SFP 1 Gbps
System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 128 GB
Odpowiedz:
Zmieniamy zapis na:
Min. 10 portami Gigabit Ethernet RJ45.
Min. 12 gniazdami SFP 1 Gbps
System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB

PYTANIE 4

6. Parametry wydajnościowe
Jest:
W zakresie Firewall'a obsługa nie mniej niż 4 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę.
Przepustowość Stateful Firewall: nie mniej niż 32 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 7 Gbps.
Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 20 Gbps.
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 11 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 6,8 Gbps.

Wyjaśnienie:
Parametry wydajnościowe wskazują platformę Fortigate FG-301E 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.
Proponowana zmiana:
W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 90.000 nowych połączeń na sekundę.
Przepustowość Stateful Firewall: nie mniej niż 30 Gbps dla pakietów generowanych przez laboratoria badające wydajność.
Przepustowość Stateful Firewall: nie mniej niż 11 Gbps dla ruchu IMIX.
Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 7 Gbps.
Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 4 Gbps.
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP – min. 11 Gbps.
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – min. 3 Gbps.

Odpowiedz:
System ma zabezpieczyć prawidłowe funkcjonowanie dużej jednostki jaką jest nasz Szpital, także w perspektywie eksploatacji przez kilka następnych lat, włącznie z przyszłymi wymaganiami dotyczącymi telemedycyny. Na rynku są urządzenia o podobnej wydajności. Dlatego Zamawiający podtrzymuje swoje wymagania.

PYTANIE 5

Wnioskujemy o wykreślenie punktu 6.
Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 6.8 Gbps.
Odpowiedz: Zamawiający podtrzymuje zapisy.

7. 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.

Wyjaśnienie:
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.

Proponowana zmiana:
4.Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS. …
7.Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. …
Odpowiedź:
4. Ochrona przed malware
Na rynku co najmniej kilku producentów oferuje funkcje ochrony przed malware dla wskazanych protokołów bezpośrednio na platformie lub pośrednio z wykorzystaniem protokołu icap (SonicWall, ForcePoint, Hilstone, Checkpoint, Fortinet.
Zamawiający podtrzymuje zapisy

Pkt 7 Zamawiający wyraża zgodę na zmianę:
7.Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. …

Wnioskujemy 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. …

Odpowiedź:
Pkt 9. Zamawiający wyraża zgodę na usunięcie punktu.
Pkt. 10. Zamawiający podtrzymuje wymaganie uwierzytelniania dwu-składnikowego z uwagi na konieczność szczególnej ochrony dostępu do strategicznych zasobów i elementów infrastruktury. Większość dostępnych na rynku rozwiązań typu Firewall oraz VPN obsługuje ten mechanizm bezpośrednio na systemie Firewall lub w połączeniu z zewnętrznym systemem uwierzytelniania dwu-składnikowego za pośrednictwem protokołu RADIUS. W przypadku kiedy mechanizm nie jest dostępny lokalnie na systemie koniecznym jest dostarczenie zewnętrznego modułu uwierzytelniania dwu-składnikowego z dwoma tokenami sprzętowymi lub programowymi z opcją rozbudowy ilości tokenów

PYTANIE 6

9. Połączenia VPN
Jest:
Pracę w trybie Portal gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0
Wyjaśnienie:
Istotne jest aby system umożliwiał pracę w trybie Portal gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki.

Proponowana zmiana:
Pracę w trybie Portal gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki.
Odpowiedz:
Zamawiający podtrzymuje wymaganie. Jednocześnie podkreśla, że dostęp SSL VPN w oparciu o HTML5 jest realizowany przez wielu producentów.

PYTANIE 7

10. Routing i obsługa łączy WAN
Jest:
W zakresie routingu rozwiązanie powinno zapewniać obsługę:
• Protokołów dynamicznego routingu w oparciu o
protokoły: RIPv2, OSPF, BGP oraz PIM.

Wyjaśnienie:
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. Statyczny routing multikastów w zupełności powinien być wystarczający na urządzeniu brzegowym. PIM jest cechą charakterystyczna dla urządzenia Fortigate firmy Fortinet.
Wnioskuejmy o usunięcie zapisu dotyczącego dynamicznego protokołu PIM.

Proponowana zmiana:
W zakresie routingu rozwiązanie powinno zapewniać obsługę:
• Protokołów dynamicznego routingu w oparciu o
protokoły: RIPv2, OSPF, BGP.
Odpowiedz:
Obsługa protokołu PIM jest realizowana przez wielu producentów rozwiązań.
Istotnym wykorzystaniem multicastu w sieciach komercyjnych jest dystrybucja plików, w szczególności dostarczanie obrazów systemu operacyjnego i aktualizacje zdalnych komputerów. Kluczową zaletą rozsyłania obrazów rozruchowych przez multicast nad rozsyłaniem Unicast jest znacznie niższe wykorzystanie przepustowości sieci. Dodatkowo protokół jest wykorzystywany w przypadku transmisji multimedialnych, które są podstawą rozwijanej obecnie telemedycyny.
Zamawiający podtrzymuje wymaganie.

PYTANIE 8

13. Ochrona przed atakami
Jest:
Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
Wyjaśnienie:
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.

Proponowana zmiana:
Baza sygnatur ataków powinna zawierać minimum 1500 wpisów, chronić przed minimum 5 000 zagrożeniami *i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.*
Odpowiedz:
Zamawiający dopuści rozwiązanie, które będzie analizowało komunikację sieciową zbiorem co najmniej 5000 sygnatur, którego skuteczność będzie udokumentowana wynikami testów prowadzonych przez NSS Labs. Zamawiający nie precyzuje w jaki sposób mechanizmy mają być implementowane w platformie jak również nie ocenia który sposób implementacji jest lepszy. Opiera się w tym zakresie na wynikach NSS Labs, które prezentują skuteczność ochrony przed atakami, w tym również wydajność dla wielu specjalizujących się w bezpieczeństwie producentów: m.in. Checkpoint, Fortinet, Paloalto, McAffe, TrendMicro. Zamawiający podtrzymuje wymaganie.

PYTANIE 9

14. Kontrola aplikacji
Jest:
Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
Wyjaśnienie:
Zgodnie z wyjaśnieniem dotyczącym punktu 13. – kontrola aplikacji w innych systemach również robione są poprzez mechanizm IPS.
Proponowana zmiana:
Baza Kontroli Aplikacji powinna zawierać minimum 330 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora
Odpowiedz:
Zamawiający podtrzymuje wymaganie ilości aplikacji. Wiele produktów na rynku dostarcza aktualizowanej listy kilku tysięcy aplikacji. Duża baza sygnatur pozwala definiować granularne polityki w zakresie analizy ruchu sieciowego.

PYTANIE 10
15. Kontrola WWW
Jest:
W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
…
System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
Wyjaśnienie:
Cecha te są charakterystyczna dla urządzenia Fortigate firmy Fortinet. Zaś ochrona z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, … jest realizowana poprzez inną funkcjonalność zananą pod nazwą IP Reputation.

Wnioskujemy o wykreślenie:
W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
…
System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
Odpowiedz:
Zamawiający wyraża zgodę na wykreślenie powyższych sformułowań.

PYTANIE 11

16. Uwierzytelnianie użytkowników w ramach sesji
Jest:
Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu – składnikowego
Wyjaśnienie:
Patrz wyjaśnienie, punkt 7 podpunkt 10.
Wnioskujemy o wykreślenie:
Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu – składnikowego
Odpowiedz:
Zamawiający podtrzymuje wymaganie uwierzytelniania dwu-składnikowego dla sesji firewall. Zostało pomówione w p.10. Zastosowanie mechanizmów jest istotne z punktu widzenia ochrony dostępu do zasobów, w których przechowywane są dane wrażliwe.

PYTANIE 12

19. 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

Wyjaśnienie:
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 instytucję publiczną, która funkcjonuje w kraju członkowskim Unii Europejskiej i NATO, stąd powinien raczej wymagać certyfikacji, 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.

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

Odpowiedz:
Zamawiający wyraża zgodę na zmianę.

PYTANIE 13

21. Ochrona typu sandbox
Jest:
System proaktywnej ochrony przed zaawansowanymi zagrożeniami - którego zadaniem będzie wykrywanie i blokowanie ataków w infrastrukturę sieci a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń.
System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji. System powinien być dostarczony w postaci komercyjnej platformy działającej w środowisku wirtualnym z możliwością uruchomienia na co najmniej
następujących hypervisorach: VMware ESXi 5.1 lub nowsze, Citrix XenServer 6.2 lub nowsze.
System powinien umożliwiać lokalne logowanie oraz raportowanie oraz współpracować z systemem centralnego logowania i raportowania. Powinna istnieć możliwość implementacji systemu w trybie nasłuchu oraz współpracy z systemami zabezpieczeń NGFW (Next Generation Firewall) lub SWG (Security Web Gateway), SEG (Secure Email Gateway) oraz w oparciu o interfejsy programistyczne API (np. icap).
Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcia i aktualizacji oprogramowania.
Dla zapewnienia wysokiej sprawności i skuteczności działania elementy systemu muszą pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.
Nie mniej niż 6 portów Ethernet 10/100/1000.
Powierzchnia dyskowa - minimum 4 TB
W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability) z podziałem obciążenia. Ochrona przez zaawansowanymi atakami:
Funkcjonalność Sandbox dla instancji Windows: sprawdzanie procesów i rejestru, połą
czenia z Botnet C&C oraz złośliwymi URL, dostęp do pakietów przeprocesowanych przez VM, logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM.
Procesowanie plików o rozmiarze co najmniej 8 MB.
Sanboxing dla plików zarchiwizowanych (.tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj), wykonywalnych (.exe, .dll), PDF, Windows Office Document,
Javascript, AdobeFlash oraz JavaArchive (JAR)
Plików multimedialnych: .avi, .mpeg, .mp3, .mp4

Skanowane protokoły sieciowe: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM oraz ich wersje zaszyfrowane SSL. Jeżeli do spełnienia tego wymagania konieczne jest dostarczenie dodatkowych urządzeń sieciowych (przekierowujących zawartość pakietów dla wskazanych protokołów sieciowych, rozszywających ruch SSL), urządzenia te powinny zostać uwzględnione w ofercie. Ich wydajność powinna umożliwiać procesowania ruchu o przepływności 1 Gbps.
Skanowanie stron www z linkami URL
Czarne i białe listy dla sum kontrolnych plików
Szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci, snapshotu VM.
Dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap.
Możliwość uruchomienia min. 4 instancji wirtualnych systemów MS Windows zawierających Windows 7, Windows 8 i Windows 10 oraz pakiet biurowy MS Office w celu wykonania analizy Sandbox w wymiarze co najmniej 70 plików na godzinę.
System udostępnia:
Lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS
Dostęp do CLI przez SSH
Wymaga się aby dostawa obejmowała również:
Gwarancję i serwis producenta na okres 36 mcy
Subskrypcje funkcji bezpieczeństwa na okres: 36 mcy
Rozwiązanie musi zostać uruchomione i skonfigurowane na trzech serwerach terminalowych pracujących u Zamawiającego.

Wyjaśnienie:
Opisane parametry wskazują platformę FortiSandbox firmy Fortinet. Żaden inny producent nie jest w stanie spełnić wszystkich wymagań łącznie. Poniżej przedstawiamy parametry, które zapewnią wydajny i bezpieczny moduł sandboxingu w oparciu o chmurę producenta, w której pracuje wydajna farma serwerów z zaawansowanymi technologiami Sandbox, oraz bezpośrednie wsparcie zespołu inżynierów R&D.

Proponowana zmiana:
System proaktywnej ochrony przed zaawansowanymi zagrożeniami - którego zadaniem będzie wykrywanie i blokowanie ataków w infrastrukturę sieci a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń.

System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji. System powinien być dostarczony w postaci komercyjnego wsparcia typu Sandbox.

System powinien umożliwiać logowanie oraz raportowanie oraz współpracować z systemem centralnego logowania i raportowania.
Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcia i aktualizacji oprogramowania.

Dla zapewnienia wysokiej sprawności i skuteczności działania elementy system musi pracować w oparciu o chmurę z co najmiej dwoma centrami data center.

Funkcjonalność Sandbox dla instancji Windows: sprawdzanie procesów i rejestru, połączenia z Botnet C&C oraz złośliwymi URL, przez VM.

Sanboxing dla plików zarchiwizowanych (.tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR)

Skanowane protokoły sieciowe: HTTP, SMTP, POP3, FTP, oraz ich wersje zaszyfrowane SSL. Jeżeli do spełnienia tego wymagania konieczne jest dostarczenie dodatkowych urządzeń sieciowych (przekierowujących zawartość pakietów dla wskazanych protokołów sieciowych, rozszywających ruch SSL), urządzenia te powinny zostać uwzględnione w ofercie. Ich wydajność powinna umożliwiać procesowania ruchu o przepływności 1 Gbps.

Wsparcie producenta dla Sandboxing na okres 36 mcy

Subskrypcje funkcji bezpieczeństwa dla Sandboxing na okres: 36 mcy

Rozwiązanie musi zostać uruchomione i skonfigurowane.

Odpowiedź:

Jakiekolwiek rozwiązania wykorzystujące chmurę publiczną do obróbki i przechowywania niezaszyfrowanych danych są nie do wykorzystania w zakresie systemów przetwarzających dane osobowe wrażliwe, a więc dane medyczne, co ma miejsce u Zamawiającego. Opisane przez Zamawiającego rozwiązanie może być innego producenta niż firewall, lecz musi być z nim zintegrowane. Takie rozwiązania, zarówno różnych, jak i tego samego producenta są dostępne na rynku. Zamawiający nie wyraża zgody na zmiany.

PYTANIE 14

Dotyczy:

TABELA NR II
Punkt 2. Ochrona przed atakami – w ramach standardowej licencji funkcji ochronnych IPS.
Jest:

a) bez dodatkowych opłat lub licencji rozszerzonych, możliwość poszerzenia bazy sygnatur ataków do
minimum 10000 w celu skuteczniejszej ochrony wrażliwych systemów /25pkt/
b) za dodatkową opłatą lub licencją rozszerzoną, możliwość poszerzenia bazy sygnatur ataków dominimum 10000 w celu skuteczniejszej ochrony wrażliwych systemów.
/12/

Wyjaśnienie:
Zgodnie z wyjaśnieniami dotyczącymi: TABELA NR I, punkt 13. Ochrona przed atakami, chcielibyśmy zaznaczyć, że nie tylko większa ilość sygnatur oznacza ochronę przed większą ilością zagrożeń. W przypadku technologii dostępnych w Polsce, 1 500 sygnatur może chronić przed 10 000 zagrożeń.
Proponowana zmiana:

a) bez dodatkowych opłat lub licencji rozszerzonych, możliwość poszerzenia bazy sygnatur ataków do takiej liczby, żeby zapewniona była ochrona przed minimum 10 000 zagrożeń w celu skuteczniejszej ochrony wrażliwych systemów. /25pkt/

b) za dodatkową opłatą lub licencją rozszerzoną, możliwość poszerzenia bazy sygnatur ataków do takiej liczby, żeby zapewniona była ochrona przed minimum 10 000 zagrożeń w celu skuteczniejszej ochrony wrażliwych systemów.
/12 pkt/

Odpowiedz:
Zamawiający nie wyraża zgody na zmiany

W załączeniu do niniejszego pisma
Zmieniony Załącznik Nr 2 do SIWZ pn. ,,Opis przedmiotu zamówienia/Parametry techniczne".
Wykonawcy są zobowiązani składać oferty na zmienionym Załączniku Nr 2 do SIWZ.

Termin, miejsce składania i otwarcia ofert nie ulegają zmianie.
Składanie ofert: do dnia **29 maja 2018 r. do godziny 13:00.**
Otwarcie ofert odbędzie się tego samego dnia o godzinie 13:15 w Dziale Zamówień Publicznych w pokoju 3.29.
Miejsce składania ofert, określone w Specyfikacji Istotnych Warunków Zamówienia, pozostaje bez zmian.

Z poważaniem

Z upoważnienia Dyrektora
Wojewódzkiego Szpitala Specjalistycznego
im. Najświętszej Maryi Panny w Częstochowie

dr n. med. Janusz Kapustecki

Zmieniony ZALĄCZNIK NR 2 DO SIWZ
Znak sprawy: **DAZ.26.038.2018 r.**
ZAŁĄCZNIK NR 1 DO UMOWY

OPIS PRZEDMIOTU ZAMÓWIENIA / PARAMETRY TECHNICZNE

Przedmiot zamówienia: **Dostawa firewalla dla Wojewódzkiego Szpitala Specjalistycznego im. Najświętszej Maryi Panny w Częstochowie wraz z wymianą firewalla, konfiguracją oraz szkoleniem pracowników.**

FIREWALL – 1 sztuka.

I. Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
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.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.

Warunki udziału:

1. W przypadku importu rozwiązania, Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.), czyli oświadczenie odbiorcy towaru podwójnego zastosowania zgodnie z załączonym wzorem, oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora
3.]producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

TABELA NR I.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Wymagane	Oferowane
1.	Producent:	Proszę podać:	**TAK**	
2.	Nazwa i typ produktu:	Proszę podać:	**TAK**	

3.	Informacje ogólne	Rozwiązanie musi być dostępne jako platforma sprzętowa. Urządzenie jest nielimitowane na użytkowników. Urządzenie musi być fabrycznie nowe.	**TAK**	
4.	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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.	**TAK**	
5.	Parametry sprzętowe	System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45. 12 gniazdami SFP 1 Gbps. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. System musi być wyposażony w zasilanie AC. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.	**TAK**	
6.	Parametry wydajnościowe:	W zakresie Firewall'a obsługa nie mniej niż 4 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 32 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 7 Gbps. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 20 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 11 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 6.8 Gbps.	**TAK**	
7.	Funkcje Systemu Bezpieczeństwa:	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.	**TAK**	

		8. Zarządzanie pasmem (QoS, Traffic shaping). 9. 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. 10. Analiza ruchu szyfrowanego protokołem SSL. 11. Analiza ruchu szyfrowanego protokołem SSH.		
8.	Polityki, Firewall	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	**TAK**	
9.	Połączenia VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.	**TAK**	
10.	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.	**TAK**	
11.	Zarządzanie pasmem	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	**TAK**	

12.	Kontrola Antywirusowa	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą typu Sandbox opisaną w punkcie 21.	**TAK**	
13.	Ochrona przed atakami	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	**TAK**	
14.	Kontrola aplikacji	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	**TAK**	
15.	Kontrola WWW	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.	**TAK**	
16.	Uwierzytelnianie użytkowników w ramach sesji	System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem	**TAK**	

		Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.		
17.	Zarządzanie	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	**TAK**	
18.	Logowanie	System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, ale w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.	**TAK**	
19.	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa muszą być certyfikowane co najmniej w zakresie: • ICSA lub EAL4 dla oferowanego urządzenia • Certyfikat ICSA lub rekomendacja respektowana przez NATO i Unię Europejską NATO Restricted i UE Restricted dla funkcji IPS, IPSec VPN, SSL VPN.		
20.	Serwisy, licencje i gwarancje	Trzy lata gwarancji producenta. Zgłaszanie awarii w dni robocze od 7 do 15. Zgłoszenia elektroniczne możliwe po godz.15 lub w dni wolne od pracy, liczone jak zgłoszone w pierwszy dzień roboczy rano. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów obejmujące Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:	**TAK**	

		• Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego. W przypadku wymiany urządzenie zamawiający musi mieć możliwość usunięcia i zachowania dysku twardego przed jego odesłaniem do dostawcy bez utraty gwarancji.		
21.	Ochrona typu sandbox	System proaktywnej ochrony przed zaawansowanymi zagrożeniami - którego zadaniem będzie wykrywanie i blokowanie ataków w infrastrukturę sieci a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji. System powinien być dostarczony w postaci komercyjnej platformy działającej w środowisku wirtualnym z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESXi 5.1 lub nowsze, Citrix XenServer 6.2 lub nowsze. System powinien umożliwiać lokalne logowanie oraz raportowanie oraz współpracować z systemem centralnego logowania i raportowania. Powinna istnieć możliwość implementacji systemu w trybie nasłuchu oraz współpracy z systemami zabezpieczeń NGFW (Next Generation Firewall) lub SWG (Security Web Gateway), SEG (Secure Email Gateway) oraz w oparciu o interfejsy programistyczne API (np. icap). Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcia i aktualizacji oprogramowania. Dla zapewnienia wysokiej sprawności i skuteczności działania elementy systemu muszą pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. Nie mniej niż 6 portów Ethernet 10/100/1000. Powierzchnia dyskowa - minimum 4 TB W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability) z podziałem obciążenia. Ochrona przez zaawansowanymi atakami: • Funkcjonalność Sandbox dla instancji Windows: sprawdzanie procesów i rejestru, połączenia z Botnet C&C oraz złośliwymi URL, dostęp do pakietów przeprocesowanych przez VM, logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM. • Procesowanie plików o rozmiarze co najmniej 8 MB. • Sanboxing dla plików zarchiwizowanych (.tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR) • Plików multimedialnych: .avi, .mpeg, .mp3, .mp4 • Skanowane protokoły sieciowe: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM oraz ich wersje zaszyfrowane SSL. Jeżeli do spełnienia tego wymagania konieczne jest dostarczenie dodatkowych urządzeń sieciowych (przekierowujących zawartość pakietów dla wskazanych protokołów sieciowych, rozszywających ruch SSL), urządzenia te powinny zostać uwzględnione w ofercie. Ich wydajność powinna umożliwiać procesowania ruchu o przepływności 1 Gbps. • Skanowanie stron www z linkami URL	**TAK**	

		• Czarne i białe listy dla sum kontrolnych plików • Szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci, snapshotu VM. • • Dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap. Możliwość uruchomienia min. 4 instancji wirtualnych systemów MS Windows zawierających Windows 7, Windows 8 i Windows 10 oraz pakiet biurowy MS Office w celu wykonania analizy Sandbox w wymiarze co najmniej 70 plików na godzinę. System udostępnia: • Lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS • Dostęp do CLI przez SSH Wymaga się aby dostawa obejmowała również: • Gwarancję i serwis producenta na okres 36 mcy • Subskrypcje funkcji bezpieczeństwa na okres: 36 mcy Rozwiązanie musi zostać uruchomione i skonfigurowane na trzech serwerach terminalowych pracujących u Zamawiającego		
22.	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwa forma elektroniczna. Dokumentacja ma być dostarczona na nośniku papierowym lub elektronicznym – nie wystarczy możliwość ściągnięcia z internetu.	**TAK**	
23.	Wdrożenia i szkolenia	Wdrożenie urządzenia w siedzibie Zamawiającego zakończone podpięciem urządzenia i zweryfikowaniem poprawności konfiguracji zgodnie z wymaganiami Zamawiającego. Musi pozwolić oprócz uruchomienia filtrowania dostępu do internetu poprzez użytkowników AD, także na jednoczesne filtrowanie po adresach IP stacji, położonych w różnych VLANach IP, przy czym konfiguracja routingu na urządzeniach w sieci Zamawiającego ma pozostać niezmieniona. Zgodnie z wymaganiami informatyków Zamawiającego, mają zostać uruchomione i skonfigurowane wszystkie elementy zakupionego pakietu – firewall, IPS, filtrowanie treści, antywirus, VPN, sandbox, itp. Szczegóły dotyczące włączenia do infrastruktury, ze względu na poufność, zostaną udostępnione Wykonawcy dopiero po podpisaniu umowy W ramach wdrożenia należy przewidzieć co najmniej 5 dni roboczych wizyt certyfikowanego inżyniera. Szkolenie dla trzech osób wykonane przez autoryzowany przez producenta ośrodek szkoleniowy na terenie kraju. Szkolenie ma być zakończone egzaminem, po którym uczestnicy otrzymają certyfikat ukończenia szkolenia. Szkolenia, w przypadku braku możliwości realizacji w trakcie wdrożenia, mogą zostać dostarczone w postaci voucherów ważnych co najmniej rok.	**TAK**	
24.	Miejce	Urządzenie ma zostać dostarczone i zamontowane w Dziale Informatyki, ul. Bialska 104./118	**TAK**	

II. Instalacja i wdrożenie winny odbywać się w godzinach pracy pracowników Zamawiającego tj. w dni robocze (od poniedziałku do piątku), w godz. 7.30-14:30. Zamawiający dopuszcza wykonywanie prac w innym czasie niż wskazany, po odpowiednim uzgodnieniu i jego akceptacji.

W trakcie realizacji projektu Szpital musi posiadać dostęp do internetu co najmniej na dotychczasowym poziomie i z co najmniej dotychczasowymi zabezpieczeniami, do momentu przejścia na pracę na nowym sprzęcie, potwierdzonym protokołem odbioru końcowego przedmiotu umowy. Wdrożenie nie może utrudnić lub uniemożliwić rozliczeń z płatnikami oraz korzystania z funkcjonalności systemu Szpitalnego.

TABELA NR II.

Lp.	Nazwa komponentu	Wymagania dodatkowo oceniane	Wymagane	Oferowane
1.	Poufność transmisji danych - połączenia szyfrowane IPSec VPNoraz SSL VPN dostarczone w modelu:	a) nielicencjonowanym–Zamawiający nie będzie ponosił dodatkowych kosztów związanych z realizacją funkcjonalności i nie jest ona licencjonowana przez Producenta oferowanego urządzenia. /15pkt/	**TAK/NIE**	
		b) licencjonowana jednorazowo, dożywotnio – Zamawiający będzie zobligowany do zakupu dodatkowych licencji jednorazowo, na zadaną liczb użytkowników lub jako jednorazowy zakup funkcjonalności dla sztuki urządzenia. /7pkt/	**TAK/NIE**	
		c) subskrypcyjnym–Zamawiający będzie zobligowany do zakupu licencji czasowej, na zadaną liczb użytkowników lub funkcjonalność dla sztuki urządzenia. /0pkt/	**TAK/NIE**	
2.	Ochrona przed atakami - w ramach standardowej licencji funkcji ochronnych IPS:	a) bez dodatkowych opłat lub licencji rozszerzonych, możliwość poszerzenia bazy sygnatur ataków do minimum 10000 w celu skuteczniejszej ochrony wrażliwych systemów. /25pkt/	**TAK/NIE**	
		b) za dodatkową opłatą lub licencją rozszerzoną, możliwość poszerzenia bazy sygnatur ataków dominimum 10000 w celu skuteczniejszej ochrony wrażliwych systemów. /12pkt/	**TAK/NIE**	
		c) brak możliwości poszerzenia bazy sygnatur ataków. /0pkt/	**TAK/NIE**	

……., dnia…… 2018 r.

……

Pieczęć imienna i podpisy osób uprawnionych
do składania oświadczeń woli
w imieniu Wykonawcy