Załącznik nr 4 do SIWZ

Minimalne wymagania dla systemu bezpieczeństwa – funkcjonalności punktowane dodatkowo, w które zostanie wyposażony ***system bezpieczeństwa*** w ciągu **1 roku** od daty dostawy

Uwagi dotycząca wypelniania tego załącznika

- W kolumnie „Funkcjonalność" zostały podane opisy dodatkowych funkcjonalności, za które Zamawiający przyzna dodatkowe punkty, jeśli zostaną one zrealizowane i dołączone do oferowanego ***systemu bezpieczeństwa*** w ciągu **1 roku** od daty jego dostawy.
- Lista tych funkcjonalności jest identyczna z listą zawartą w załączniku nr 3.
- Jeżeli Oferent chce zobowiązać się do zrealizowania danej funkcjonalności w ciągu **1 roku** od daty podpisania umowy na dostawę ***systemu bezpieczeństwa***, to w wierszu w którym wypisano daną funkcjonalność wstawia **X** wewnątrz ***** znajdującego się w kolumnie „ST".
- Każda funkcjonalność, dla której w kolumnie „ST" wewnątrz ***** wpisano znak **X** otrzyma ilość ***punktów elementarnych*** równą liczbie podanej w kolumnie „PKT" z wiersza danej funkcjonalności.
- Niektóre wymagania dotyczące funkcjonalności, mają przypisaną punktację za realizację tych funkcjonalności i jednocześnie posiadają dodatkowe uszczegółowienia funkcjonalne za których realizację otrzymuje się kolejne punkty. W takich przypadkach należy odrębnie zaznaczać ***** dla każdej funkcjonalności i jej dodatkowego uszczegółowienia funkcjonalnego.

Funkcjonalność	**PKT**	**ST**
A. VPN		
1. ***System bezpieczeństwa*** posiada funkcjonalność pozwalającą na tworzenia specjalnych kanałów VPN dedykowanych do zarządzania ***urządzeniami*** i centralną konsolą	1	*
2. ***System bezpieczeństwa*** posiada funkcjonalność pozwalającą na wymuszenie, że zestawienie tunelu VPN nastąpi dopiero po spełnieniu określonych (definiowalnych, dynamicznych) zasad bezpieczeństwa innych niż tylko weryfikacja certyfikatów	1	*
3. ***Urządzenia*** posiadają funkcjonalność pozwalającą na zestawianie tuneli SSL VPN		
a) Site-to-Site	1	*
b) Client-to-Site	1	*
4. ***System bezpieczeństwa*** posiada funkcję skanowania antyspamowego tuneli VPN (IPsec/L2TP/PPTP)	1	*
B. NAC		
1. ***System bezpieczeństwa*** zawiera mechanizm NAC	1	*
2. NAC posiada funkcje wykrywania zgodności i dostosowywania konfiguracji badanych urządzeń sieciowych do ustalonych przez administratora polityk bezpieczeństwa	1	*
3. NAC realizuje swoje funkcje bez konieczności instalowania na badanych urządzeniach klienta NAC	1	*
4. ***System bezpieczeństwa*** posiada mechanizm, za pomocą którego NAC będzie w stanie dokonać automatycznej zmiana uprawnień i ustawień sieciowych w odniesieniu do urządzeń sieciowych, które NAC zidentyfikował jako niespełniające wymagań bezpieczeństwa	1	*

Funkcjonalność	**PKT**	**ST**
C. Polityki dla portów Ethernet ***Urządzenia*** posiadają funkcjonalność pozwalającą na określenie odrębnie dla każdego portu ethernet ***urządzenia***:		
1. zachowania w przypadku		
a) odłączenia kabla od portu	1	*
b) ponownego podłączenia kabla do portu	1	*
1) z uwzględnieniem informacji o konfiguracji urządzenia sieciowego podłączanego do danego portu, w tym o adresie MAC urządzenia sieciowego	1	*
2. zasady konfiguracji w przypadku wystąpienia sytuacji opisanych w pkt. 1a muszą pozwalać na zmianę		
a) stanu portu: włączony/wyłączony	1	*
b) przypisania do ***strefy bezpieczeństwa***	1	*
D. Polityki dla portów USB ***Urządzenia*** posiadają funkcjonalność pozwalającą na określenie odrębnie dla każdego portu USB ***urządzenia***:		
1. zachowania w przypadku wystąpienia sytuacji		
a) odłączenia urządzenia USB od portu	1	*
b) ponownego podłączenia urządzenia USB do portu, z uwzględnieniem informacji o konfiguracji urządzenia USB podłączanego do danego portu, w tym o	1	*
1) typie urządzenia USB	1	*
2) modelu urządzenia USB	1	*
3) numerze seryjnym urządzenia USB	1	*
2. zasady konfiguracji w przypadku wystąpienia sytuacji opisanych w pkt. 3a muszą pozwalać na zmianę		
a) stanu portu: włączony/wyłączony	1	*
b) w przypadku modemów 3G przypisania do ***strefy bezpieczeństwa***	1	*
E. Skrypty		
1. ***Urządzenia*** posiadają funkcjonalność pozwalającą na tworzenie i uruchamianie na nim skryptów		
a) na żądanie ***operatora***	1	*
b) wg ustalonego harmonogramu	1	*
c) w odpowiedzi na zdarzenie	1	*
2. Skrypty posiadają pełny dostęp do API ***urządzenia***, w tym pozwalają na		
a) tworzenie, modyfikowanie i usuwanie ***reguł bezpieczeństwa***	1	*
b) tworzenia i zamykanie kanałów VPN	1	*
c) włączanie i wyłączanie całego ***urządzenia*** oraz poszczególnych komponentów sprzętowych, w tym w szczególności portów ethernetowych, USB oraz WiFi	1	*
d) odczytywanie informacji o		
1) bieżącej utylizacji komponentów sprzętowych,	1	*
2) wydajności urządzenia i jego modułów	1	*
3) wynikach działania ***reguł bezpieczeństwa***	1	*
e) dostęp do modułu NAC, w tym definicji i zdarzeń generowanych wskutek uruchomienia ***reguł bezpieczeństwa*** dostępu do sieci lub działania mechanizmów przystosowujących konfigurację badanych przez NAC urządzeń do ustalonych przez administratora polityk bezpieczeństwa	1	*
1) wynikach badania obecności innych urządzeń sieciowych	1	*
F. Integracja z innymi systemami		
1. ***Urządzenia*** integrują się z ***AD*** metodą bezpośredniej komunikacji z kontrolerem domeny, bez konieczności wykonywania importu kont użytkowników i grup	3	*
2. ***Urządzenia*** posiadają funkcjonalność tworzenia reguł zezwalających na zalogowanie na podstawie adresów MAC	3	*

Funkcjonalność	PKT	ST
G. Sytuacje awaryjne		
1. W przypadku awarii urządzenia ***GRIO***, ***system bezpieczeństwa***, w ramach posiadanych licencji, zezwala na tymczasowe przeniesienie (tj. na czas awarii) ***urządzenia*** wraz z licencjami niezbędnymi do działania wszystkich jego funkcjonalności do środowiska wirtualnego bez konieczności posiadania dodatkowych licencji w stosunku do tych zawartych w ofercie	1	*
2. Wygaśnięcie licencji na subskrypcje definicji używanych przez poszczególne moduły ***aktywnej ochrony*** nie powoduje wyłączenia lub ograniczenia funkcjonalności danego modułu	1	*
H. *Reguły bezpieczeństwa*		
1. ***Urządzenia*** posiadają funkcjonalność pozwalającą na określanie harmonogramu dla aktywności poszczególnych ***reguł bezpieczeństwa***	5	*
2. ***Urządzenia*** pozwalają na zdefiniowanie kryterium ***reguły bezpieczeństwa*** w oparciu o źródłowe i docelowe		
a) adresy MAC	16	*
b) grupy vlan	8	*
3. ***System bezpieczeństwa*** posiada mechanizm weryfikacji poprawności definicji ***reguł bezpieczeństwa***	10	*
I. *QoS*		
1. ***Urządzenia*** pozwalają na zdefiniowanie polityki QoS w oparciu o:		
a) protokoły sieciowe	1	*
b) dla każdą ze stref bezpieczeństwa	1	*
c) źródłowe i docelowe adresy IP	1	*
d) źródłowe i docelowe grupy vlan	1	*
e) kategorię web	1	*
J. *MKSI* Moduł ***MKSI*** każdego urządzenia posiadają funkcjonalność pozwalającą na:		
1. na ograniczanie wykorzystania pasma (QoS) podczas otwierania stron należących do każdej kategorii stron w sposób niezależny od ustawień reguł firewalla	1	*
2. wdrożenie strategii „***szarej listy***" polegającej na sprawdzeniu przez ***system bezpieczeństwa*** czy strona nie znajduje się na liście stron dozwolonych lub że jest liście stron niedozwolonych i w przypadku wystąpienia jednej z tych sytuacji, przekazaniu użytkownikowi informacji o tym fakcie i wymuszeniu na nim podjęcia decyzji czy chce wejść na taką stronę czy też nie. Decyzja użytkownika jest zapisywana w logach a treść komunikatu jest definiowana przez administratora ***system bezpieczeństwa***	15	*
a) funkcjonalność ***szarej listy*** jest realizowana z wykorzystaniem stron zdefiniowanych w białych listach (dla wykrywania prób wejścia na strony, które nie są określone jako strony dozwolone) i czarnych listach (dla wykrywania prób wejścia na strony, które są określone jako strony niedozwolone)	5	*
3. definiowanie reguł przypisywania stron do kategorii i rodzaju listy na podstawie słów kluczowych, polegającą na wyszukiwaniu na stronie wybranych słów i użycia takiego algorytmu, który na podstawie ilości i wagi znalezionych na stronie słów kluczowych dokonuje przypisania strony do odpowiedniej kategorii stron	1	*
4. wyświetlanie w miejscu zablokowanej części strony informacji o treści konfigurowanej przez administratora	1	*
a) dla każdej kategorii zablokowanej treści wyświetlana jest informacja o odrębnej treści	1	*
5. zawierać lokalną bazę kategorii stron – ***system bezpieczeństwa*** nie może wysyłać zapytań do zewnętrznych baz danych	1	*
K. *MAV*		
1. ***Urządzenia*** posiadają tryb pracy jako SMTP Proxy	1	*

Funkcjonalność	PKT	ST
L. *MAS*		
1. ***Urządzenia*** pozwalają blokować spam przesyłany w postaci plików graficznych	1	*
2. ***System bezpieczeństwa*** obsługuje mechanizm kwarantanny pozwalający		
a) na umieszczanie w niej wiadomości ze spamem	1	*
b) użytkownikom na przeglądanie wiadomości znajdujących się w kwarantannie	1	*
c) na podjęcie decyzji, odrębnie dla każdej wiadomości, o jej		
1) skasowaniu z kwarantanny	1	*
2) przekazaniu do komputera użytkownika.	1	*
M. Protokoły szyfrowane		
1. ***system bezpieczeństwa*** obsługuje skanowanie antywirusowe protokołów		
a) SMTPs	5	*
b) POP3s	4	*
c) IMAPs	5	*
2. ***system bezpieczeństwa*** obsługuje skanowanie antyspamowe protokołów		
a) SMTPs	5	*
b) POP3s	4	*
c) IMAPs	5	*
3. ***system bezpieczeństwa*** pozwala na włączenie/wyłączenie odrębnie dla każdej reguły bezpieczeństwa skanowania		
a) antywirusowego dla tych protokołów, które Oferent wskazał w podpunktach punktu 1, że są one obsługiwane w zakresie skanowania antywirusowego	5	*
b) antyspamowego dla tych protokołów, które Oferent wskazał w podpunktach punktu 2, że są one obsługiwane w zakresie skanowania antyspamowego	5	*
N. Konsola centralnego zarządzania		
1. przechowuje kopie firmware'ów każdego z ***urządzeń***	1	*
2. posiada funkcję zdalnej zamiany firmware'ów ***urządzeń*** na wersje znajdujące się w centralnej konsoli	1	*
3. posiada funkcję automatyczne wykonywanie kopii zapasowej konfiguracji ***urządzeń***	1	*
O. Zdarzenia sprzętowe		
1. ***system bezpieczeństwa*** posiada funkcję monitorowania w czasie rzeczywistym temperatury ***urządzeń***	1	*
2. rejestrator zdarzeń systemowych posiada zdolność logowania następujących zdarzeń związanych z pracą ***urządzeń***		
a) przekroczenie progu alarmowego dla		
1) obciążenia CPU	1	*
2) temperatury CPU	1	*
3) wykorzystania pamięci RAM	1	*
4) obciążenia interfejsów sieciowych	1	*
5) prędkości obrotowej wiatraków	1	*
b) podłączenie i odłączenie		
1) kabla do portu Ethernet	1	*
i) wraz z podaniem adresu MAC urządzenia	1	*
2) urządzenia USB	1	*
i) wraz zapisaniem informacji o typie, modelu i numerze seryjnym urządzenia USB w takim samym zakresie w jakim Oferent wskazał, że są realizowane one w podpunktach punktu D1b	1	*
3. w sytuacji wystąpienia zdarzeń opisanych w pkt.2 zdarzeń system posiada funkcję		
a) powiadamiania o nich administratorów poprzez		
1) alerty SNMP	1	*
2) e-maile	1	*
b) dynamicznego zmieniania reguł bezpieczeństwa	1	*

Funkcjonalność	PKT	ST
P. Obsługa logów		
1. ***system bezpieczeństwa*** wspiera		
a) przynajmniej 3 implementacje serwera syslog	1	*
b) zbieranie logów z innych urządzeń zgodnych z syslog	1	*
Q. Mechanizm raportowania		
1. posiada następujące raporty zbiorcze o		
a) wielkości transferu (łącznego, przychodzącego, wychodzącego)	1	*
b) ilości sesji	1	*
c) ilości i wielkości ruchu generowanego przez aplikacje, użytkowników i hosty	1	*
d) najczęściej otwieranych stronach internetowych	1	*
e) typach ruchu sieciowego, aplikacjach, użytkownikach i hostach generujących największy ruch sieciowy	1	*
2. posiada raporty zbiorcze dla całego systemu bezpieczeństwa, tj. pochodzących ze wszystkich ***urządzeń*** i modułów ***aktywnej ochrony***	1	*
3. udostępnia metodę analizowania danych zawartych w raportach zbiorczych techniką drill-down przynajmniej 3 poziomy wgłąb	5	*
a) o generowanym ruchu sieciowym	1	*
b) o pracy samego systemu	1	*
c) 5 poziomów wgłąb	3	*
4. pozwala na wyświetlanie raportu na podstawie danych dotyczących przedziału czasu, którego ramy czasowe będą podawane z dokładnością do 1 minuty	1	*
5. pozwala na		
a) definiowanie własnych raportów	1	*
b) wysyłanie raportów na pocztę elektroniczną	1	*
R. Funkcje sieciowe		
1. ***Urządzenia*** obsługują:		
a) multipath routing	1	*
b) współpracują z usługami dynamic DNS udostępnianymi przez		
1) NO-IP	3	*
2) producenta ***system bezpieczeństwa***	1	*
2. ***Urządzenia*** posiadają funkcjonalność podziału łącza w oparciu o wirtualne drzewa decyzyjne dla każdego z użytkowników z osobna lub dla grup użytkowników oraz ustawiania priorytetów (traffic shaping)	1	*
3. ***Urządzenia*** dla ***GRIO*** pozwalają na		
a) stworzenie dedykowanego linku, służącego tylko do monitorowania stanu partnera w klastrze High Availability	1	*
b) łączenie wielu kart sieciowych w jedną logiczną kartę sieciową w celu zwiększenia przepustowości	1	*
4. ***Urządzenia*** dla ***ZRIO*** pozwalają na		
a) funkcję skonfigurowania przynajmniej jednego portu Ethernet na potrzeby pracy ***urządzeń*** w trybie HA	1	*
b) stworzenie dedykowanego linku, służącego tylko do monitorowania stanu partnera w klastrze High Availability	1	*
c) łączenie wielu kart sieciowych w jedną logiczną kartę sieciową w celu zwiększenia przepustowości	1	*
5. ***Urządzenia*** dla ***IRIO*** pozwalają na skonfigurowanie każdego z portów Ethernet do pracy jako WAN, LAN, DMZ”	1	*
6. ***Urządzenia*** posiadają watchdog’i sprawdzające w czasie rzeczywistym status działania usług, stanu łącz internetowych, statusu switchy obsługujących SNMP	3	*

Funkcjonalność	**PKT**	**ST**
S. Zarządzanie *systemem bezpieczeństwa* System centralnego zarządzania posiada funkcjonalność pozwalającą na:		
1. aktualizację i zmianę systemu poprzez TFTP	1	*
2. zbudowanie hierarchicznej struktury zarządzania bezpieczeństwem VPN	1	*
3. tworzenie obiektów globalnych, tj. obiektów, które można wykorzystywać w każdym module ***aktywnej ochrony*** przy definiowaniu ***reguł bezpieczeństwa***	1	*