Załącznik nr 1 do SIWZ
spr. nr 66/BŁiI/17/UM/PMP

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa urządzeń i oprogramowania wraz z wdrożeniem na potrzeby rozbudowy, modernizacji i podniesienia bezpieczeństwa sieci LAN policyjnych ośrodków Przetwarzania Danych

SPIS TREŚCI

1. Słowniki i skróty

Dla potrzeb niniejszego opracowania przyjmuje się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Awaria	Pojęcie awarii obejmuje zarówno awarię Urządzeń, jak i awarię Oprogramowania uniemożliwiającą dalsze poprawne działanie Urządzeń.
CPD	Centrum Przetwarzania Danych jest to obiekt lub jego część, która w ramach swojej podstawowej funkcji mieści w szczególności pomieszczenie komputerowe i strefy je obsługujące.
Dokumentacja	Oznacza dokumentację wykonaną przez Wykonawcę i dostarczoną Zamawiającemu w ramach realizacji Umowy, podlegająca zatwierdzeniu przez Zamawiającego, materiały w formie papierowej, jak również informacje zapisane na innych nośnikach, w tym nośnikach elektronicznych, w szczególności: Plan Zarządzania Projektem, Projekt Techniczny, Dokumentacja Powykonawcza, Dokumentacja Eksploatacyjna, Wykaz Ilościowo-Cenowy.
Infrastruktura	Urządzenia, będące w posiadania Policji zostały opisane w punkcie 4.
Lokalizacja	Oznacza wskazane przez Zamawiającego miejsca na terytorium Warszawy, do których Wykonawca dostarczy wymagane przez Zamawiającego w ramach dostaw Urządzenia.
Nadzór Autorski	Czynności Wykonawcy wykonywane w ramach Zleceń polegające na doradztwie oraz pracach związanych z rozbudową, usprawnieniami oraz zmianą konfiguracyjną Systemu, a także dokonywanie zmiany, usprawnień lub zmian Dokumentacji, zgodnie z oczekiwaniami Zamawiającego wraz z przeniesieniem autorskich praw majątkowych oraz prawa do zezwalania na wykonywanie praw zależnych do zmienionej Dokumentacji.
Oprogramowanie	Oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty (w szczególności systemowe, bazodanowe, pomocnicze), będące przedmiotem sprzedaży i dostarczenia w ramach realizacji przedmiotu zamówienia, którego producentem jest Wykonawca lub podmiot trzeci, w tym wyższe wersje (update/upgrade), patche i programy korekcji błędów Oprogramowania Standardowego.
System	Oznacza system zaktualizowany w wyniku realizacji Umowy, w którego skład wchodzą w szczególności Urządzenia i Oprogramowanie oraz Infrastruktura.
Urządzenia	Sprzęt teleinformatyczny wraz z zawartym w nim Oprogramowaniem, niezbędnym wyposażeniem i odnoszącą się do niego dokumentacją techniczną producenta będący przedmiotem niniejszego zamówienia.

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

2. Cel Zamówienia

Przedmiot zamówienia polega na doposażeniu sprzętowo-programowym istniejącej infrastruktury sieci LAN i podniesienie bezpieczeństwa Centrów Przetwarzania Danych celem zapewnienia niezawodności i wysokiej dostępności realizowanych usług.

Poprzez zakup Urządzeń oraz Oprogramowania planuje się również zwiększenie wydajności Systemu do planowanego obciążenia.

3. Zakres zamówienia

Etapy	Przedmiot zamówienia	Maksymalny czas wyznaczony do realizacji Etapu	Minimalny czas wymagany do realizacji poszczególnych zadań w ramach Etapu
Etap 1	• Dostawa Urządzeń, licencji i oprogramowania. W ramach dostaw wymagane jest dostarczenie: o Przełączniki dostępowe sieci LAN – 12 szt. o Routery – 8 szt. o Urządzenia pełniące funkcje ściany ogniowej i bramy VPN- 8 szt. o System zarządzania urządzeniami pełniącymi funkcję ściany ogniowej bramy VPN – 1szt. o System telemetrii sieciowej wykrywania zagrożeń i ataków – 1 kpl. o System uwierzytelnienia dostępu do sieci LAN/WLAN/VPN – 1 kpl. o Środowisko serwerowe na potrzeby systemów zarządzania – 1 kpl. — Oprogramowanie do backupu — Serwery hiperkonwergentne — Oprogramowanie do wirtualizacji — Pamięć masowa do przechowywania backupu o Monitor – 1 szt. o Konsola administracyjna – 2 szt. o pamięci RAM do urządzenia UCS - 6 szt. o Moduły GBIC – 12 szt. o Urządzenie nowej generacji pełniące funkcję ściany ogniowej oraz wykrywania i zapobiegania włamaniom – 2 szt.	**40 dni od dnia podpisania Umowy,**	2 Dni Robocze na akceptację przez Zamawiającego
Etap 2	1) Przygotowanie Projektu Technicznego zawierającego w szczególności: a) Analizę aktualnego środowiska sprzętowo programowego CPD b) Plan Wdrożenia c) Konfigurację Docelową Urządzeń 2) Przygotowanie Planu Zarządzania Projektem	**40 dni od dnia podpisania Umowy**	10 Dni Roboczych na akceptację przez Zamawiającego

	3) Przygotowanie planu i opisu instruktażu z zakresu wdrażanych technologii, urządzeń i oprogramowania 4) Przeniesienie na Zamawiającego autorskich praw majątkowych do Dokumentacji wytworzonej w ramach etapu 2		
Etap 3	1) Wykonanie usługi wdrożeniowej, optymalizacyjnej szczegółowo opisanych w punktach 11 i 12.	**do dnia 8 grudnia 2017 roku**	10 Dni Roboczych na czynności odbiorcze po stronie Zamawiającego
Etap 4	1) opracowanie i dostarczenie Dokumentacji Powykonawczej, Dokumentacji Eksploatacyjnej oraz Wykazu Ilościowo-Cenowego; 2) przeniesienie na Zamawiającego autorskich praw majątkowych do Dokumentacji wytworzonej w ramach Etapu 4;	**do dnia 8 grudnia 2017 roku**	5 Dni Roboczych na czynności odbiorcze po stronie Zamawiającego
Instruktaż	1) instruktaż wdrożeniowy z zakresu konfiguracji i administrowania dostarczonymi Urządzeniami, technologiami lub platformami sprzętowymi, realizowany na Zlecenie Zamawiającego;	**do dnia 8 grudnia 2017 roku**	3 Dni Robocze na czynności odbiorcze po stronie Zamawiającego dotyczące każdorazowego odbioru Zlecenia.
Gwarancja	1) świadczenie Usług Gwarancyjnych na zasadach szczegółowo opisanych w punkcie 9.	**od dnia podpisania Protokołu Odbioru Etapu 3**	3 Dni Robocze na akceptację przez Zamawiającego

4. **Opis Środowiska Zamawiającego:**

Aktualne środowisko sieciowe oparte jest na urządzeniach Cisco serii 3550, 3560, 3750, 3800, 6800, 6500, Nexus 7k, Nexus 5k, Routery ASR 1002, 3900, 3800, firewalle ASA 5585, 5525, 5520 z kartami IPS. System zarządzania zamawiającego realizowany jest za pomocą oprogramowania CISCO Prime Infrastructure 3.1, Cisco LMS 4.2.5, CSM, DCMN, Cisco Firepower Management Center, Juniper STRM. W infrastrukturze sieciowej wykorzystywane są między innymi protokoły sieciowe i rozwiązania: EIGRP, STP, FabricPath. Ponadto infrastruktura sieciowa jest umieszczona w dwóch ośrodkach CPD połączonych za pomocą czterech łączy każde po 10 Gb. W środowisku zamawiającego, przez użytkownika końcowego używane są następujące systemy operacyjne: Windows XP, Vista, 7, 8, 10, Mac OS X, Linux/Unix.

5. **Wymagania ogólne**

a. Wszystkie parametry podane w wymaganiach są wymaganiami minimalnymi, jakie winny spełniać Urządzenia.
b. Urządzenia oraz Oprogramowanie winny zostać zamontowane oraz skonfigurowane w obiektach KGP wskazanych przez Zamawiającego zgodnie z wymaganiem szczegółowo opisanym w punktach 11 i 12. Środowisko sieciowe Zamawiającego zostało opisane w punkcie 4.
c. Jeżeli nie są wyszczególnione specyficzne warunki świadczenia usług gwarancyjnych obowiązujące wymagania minimalne przedstawia punkt 9.
d. Jeżeli nie nadmieniono to należy uznać, że wszystkie Urządzenia powinny być dostarczone wraz z Oprogramowaniem.
e. Dodatkowo jeśli nie wskazano to należy uznać, że wszystkie Urządzenia powinny być dostarczone wraz z niezbędnym do instalacji Urządzeń okablowaniem.
f. O ile inaczej nie zaznaczono, wszelkie zapisy zawierające parametry techniczne należy odczytywać jako parametry minimalne.
g. Wykonawca w celu dostępu do serwerowni winien okazać poświadczenie dostępu do informacji niejawnych co najmniej o klauzuli poufne dla wszystkich pracowników wchodzących na teren serwerowni lub zaświadczenie o niekaralności.
h. Oferowane produkty nie mogą znajdować się na liście urządzeń, dla których ogłoszono informację o terminie zakończenia produkcji lub datę zaprzestania świadczenia wsparcia.
i. Zaproponowane przez Wykonawcę urządzenie musi posiadać autoryzowany serwis techniczny producenta na terytorium Unii Europejskiej
j. Wraz z dostarczonym sprzętem Wykonawca zobowiązany jest dostarczyć odpowiadające mu instrukcje i sterowniki producenta sprzętu.
k. Dostarczane Urządzenia muszą być w pełni kompatybilne z uruchomionymi u Zamawiającego systemami zarządzania. W przypadku braku takiej kompatybilności Wykonawca musi zapewnić system zarządzania, który zarówno obejmie nowe jak i obecnie użytkowane urządzenia przy zachowaniu dotychczasowej funkcjonalności oprogramowania zarządzającego.
l. Zamawiający wymaga przedstawienia pełnej konfiguracji dostarczanych produktów wraz z podaniem nazwy producenta i modelu urządzenia. W przypadku zaoferowania produktów równoważnych, Wykonawca wraz z ofertą powinien złożyć opis parametrów technicznych proponowanego sprzętu z podaniem nazwy producenta i modelu produktu, pozwalający zweryfikować przedstawioną ofertę ze wszystkimi minimalnymi parametrami technicznymi wymaganymi przez Zamawiającego. Z dołączonej dokumentacji musi wynikać w sposób jednoznaczny, że oferowany sprzęt spełnia minimalne parametry techniczne wymagane przez Zamawiającego. Opis

parametrów technicznych proponowanego sprzętu może mieć formę folderów, opisów technicznych, kart sprzętu itp.

m. Dopuszcza się dla uniknięcia niejednoznaczności opisów dokumentację w języku angielskim.

6. Dostarczane urządzenia i oprogramowanie

6.1. Przełącznik Dostępowy sieci LAN – 12 sztuk

Wykonawca ma obowiązek dostarczyć sprzęt nie gorszy niż wyspecyfikowany poniżej (w tabeli):

Symbol	Opis	Ilość
C1-WS3650-48TD/K9	Cisco One Catalyst 3650 48 Port Data 2x10G Uplink	1
S3650UK9-36E	CAT3650 Universal k9 image	1
PWR-C2-250WAC	250W AC Config 2 Power Supply	1
PWR-C2-250WAC/2	250W AC Config 2 Secondary Power Supply	1
CAB-TA-EU	Europe AC Type A Power Cable	2
DNA-VOUCHER	Tracker Eligibility SKU for DNA Offers	1
C1FPCAT36502K9	Cisco One Foundation Perpetual - Catalyst 3650 48-port	1
C3650-48-L-S	C3650-48 LAN Base to IP Base Paper RTU License	1
C1-PI-LFAS-2K3K-K9	Cisco ONE PI Device License for LF & AS for Cat 2k, 3k	1
C1-ISE-BASE-48P	Cisco ONE Identity Services Engine 50 EndPoint Base Lic	1
C1-EGW-50-K9	Cisco ONE Energy Mgmt Perpetual Lic - 50 DO End Points	1
C1-LC-50-1Y	Cisco ONE StealthWatch 50 FPS Lic 1 YR	1
C1F1VCAT36502-02	Tracker PID v02 Fnd Perpetual CAT36502 - no delivery	1
C3650-STACK-KIT	Cisco Catalyst 3650 Stack Module	1
C3650-STACK	Cisco Catalyst 3650 Stack Module	2
STACK-T2-50CM	50CM Type 2 Stacking Cable	1
SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	2

Wymagania minimalne w przypadku zaproponowania urządzeń równoważnych:

Rodzaj urządzenia

1. Urządzenie wielofunkcyjne pełniące rolę przełącznika sieci Ethernet
2. Przełącznik Gigabit Ethernet wyposażony w 48 portów 10/100/1000BaseT oraz 2 porty uplink 10Gigabit Ethernet SFP+ i 2 porty uplink Gigabit Ethernet SFP
3. Porty uplink muszą umożliwiać obsadzenie modułami Gigabit Ethernet SFP (co najmniej 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U) oraz 10Gigabit Ethernet (co najmniej 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, twinax) zależnie od potrzeb Zamawiającego. Wymagane jest dostarczenie dwóch modułów SFP 10G-SR-S tego samego producenta co przełącznik.

Architektura

4. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów
5. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne
6. Zainstalowany zasilacz musi zapewniać min. 250W
7. Przełącznik musi posiadać możliwość instalacji zasilacza prądu stałego
8. Przełącznik musi zapewniać możliwość rozbudowy o możliwość łączenia w stos z zapewnieniem następujących parametrów:
    a. Przepustowość w ramach stosu min. 160Gb/s
    b. Min. 9 urządzeń w stosie
    c. Zarządzanie poprzez jeden adres IP
    d. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad
9. Przełącznik musi posiadać możliwość rozszerzenia funkcjonalności o funkcję kontrolera sieci bezprzewodowej WiFi (poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych) z zachowaniem następujących parametrów:
    a. Centralne zarządzanie punktami dostępowymi zgodnie z protokołem CAPWAP (RFC 5415), w tym zarządzanie politykami bezpieczeństwa i zarządzanie pasmem radiowym (RRM)
    b. Przepustowość dla sieci WiFi nie mniejsza niż 20Gb/s
    c. Obsługa minimum 25 punktów dostępowych
    d. Obsługa minimum 1000 klientów sieci WiFi
    e. Zarządzanie pasmem radiowym punktów dostępowych:
        i. automatyczna adaptacja do zmian w czasie rzeczywistym
        ii. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
        iii. dynamiczne przydzielanie kanałów radiowych
        iv. wykrywanie, eliminacja i unikanie interferencji
        v. równoważenie obciążenia punktów dostępowych
        vi. automatyczna dystrybucja klientów pomiędzy punkty dostępowe
        vii. mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
    f. Mapowanie SSID do segmentów VLAN w sieci przewodowej:
        i. (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
        ii. tunelowanie ruchu klientów do przełącznika/kontrolera
    g. Obsługa mechanizmów bezpieczeństwa:
        i. 802.11i, WPA2, WPA
        ii. 802.1X z EAP (PEAP, EAP-TLS, EAP-FAST)
        iii. możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID
        iv. możliwość profilowania użytkowników:
            i. przydział sieci VLAN
            ii. przydział list kontroli dostępu (ACL)
        v. uwierzytelnianie punktów dostępowych w oparciu o certyfikat X.509
        vi. obsługa list kontroli dostępu (ACL)
        vii. ochrona kryptograficzna (DTLS lub równoważny) ruchu kontrolnego i ruchu użytkowników

h. Obsługa ruchu unicast i multicast IPv4:
    i. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)
    ii. obsługa konwersji ruchu multicast do unicast
i. Obsługa mobilności (roaming-u) użytkowników (L2 i L3)
j. Obsługa mechanizmów QoS
    i. 802.1p, WMM, Spec
    ii. ograniczanie pasma per użytkownik
    iii. Call Admission Control – ze statyczną definicją pasma i dynamiczną w oparciu o analizę profili ruchu
    iv. U-APSD
k. Obsługa dostępu gościnnego:
    i. przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony)
    ii. możliwość kreowania użytkowników z określeniem czasu ważności konta

10. Współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne oraz usługi bezpieczeństwa
11. Możliwość analizy ruchu pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji w warstwie 7
12. Zamawiający dopuszcza, aby funkcje przełącznika sieci Ethernet i kontrolera WLAN były realizowane na dwóch urządzeniach – w takim przypadku urządzenia muszą być połączone między sobą z wykorzystaniem dodatkowych portów 10 GE w sposób nieograniczający w żaden sposób wydajności proponowanego rozwiązania (przepustowość przełącznika przełącznik-kontroler nie mniejsza niż wydajność kontrolera)

Oczekiwana wydajność

13. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
14. Minimum 2GB pamięci DRAM i 2GB pamięci flash
15. Obsługa minimum:
    a. 1000 sieci VLAN
    b. 32.000 adresów MAC
    c. 24.000 tras IPv4

Oprogramowanie/funkcjonalność

16. Obsługa protokołu NTP
17. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
18. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree
    b. IEEE 802.1s Multi-Instance Spanning Tree
    c. Obsługa minimum 128 instancji protokołu STP
    d. Obsługa protokołu LLDP i LLDP-MED
    e. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
19. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
20. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

a. Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
g. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
i. Minimum 3000 wpisów dla list kontroli dostępu (ACE)
j. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
k. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
l. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)

21. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    b. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
    f. Kontrola sztormów dla ruchu broadcast/multicast/unicast
    g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
22. Wbudowane reflektometry (TDR) dla portów 10/100/1000
23. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 i IPv6 (minimum protokół RIP). Urządzenie musi zapewniać możliwość rozszerzenia

funkcjonalności o wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, BGP) i IPv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM, PIM-SSM) poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych

24. Obsługa protokołu HSRP/VRRP lub mechanizmu równoważnego dla usług redundancji bramy

Zarządzanie i konfiguracja

25. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)
26. Urządzenie musi zapewniać możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, Net-Flow Lite, J-Flow lub równoważne)
27. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
28. Dedykowany port Ethernet do zarządzania out-of-band
29. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
30. Urządzenie musi być wyposażone w port konsoli USB
31. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją
32. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6

Obudowa

33. Możliwość montażu w szafie rack 19". Wysokość urządzenia nie może przekraczać 1 RU

Wyposażenie

34. Oferowany przełącznik musi być wyposażony w:
    a. Zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy
    b. Moduł stakujący wraz z kablem o długości 0.5m

6.2. Routery – 8 szt.

Wykonawca ma obowiązek dostarczyć sprzęt nie gorszy niż wyspecyfikowany poniżej (w tabeli):

ASR1001X-2.5G-K9	ASR1001-X, 2.5G Base Bundle, K9, AES, Built-in 6x1G	1
SLASR1-AES	Cisco ASR 1000 Advanced Enterprise Services License	1
ASR1K-INTERNET	ASR1K-Int Edge/Peering incl. BGP/NAT/ZBFW - tracking only	1
GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	4
M-ASR1001X-8GB	Cisco ASR1001-X 8GB DRAM	1
NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400	1
SPA-BLANK	Blank Cover for regular SPA	1

SASR1K1XUK9-316S	Cisco ASR1001-X IOS XE UNIVERSAL	1
ASR1001-X-PWR-AC	Cisco ASR1001-X AC Power Supply	2
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	2

Wymagania minimalne w przypadku zaproponowania urządzeń równoważnych:

1. Urządzenie o architekturze modularnej, wyposażone w 6 portów Gigabit Ethernet przeznaczone dla modułów typu SFP (optycznych lub RJ-45) lub równoważnych, a także w 2 porty 10 Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP+ lub równoważnych.
2. Urządzenie umożliwia rozszerzenie m.in. o następujące porty:
    a. 1 port 10 GigabitEthernet
    b. 8 portów Gigabit Ethernet
    c. 4 interfejsy ATM STM1 lub 2 interfejsy STM4
3. Urządzenie umożliwia dołożenie przestrzeni dyskowej typu SSD o pojemności do 400 GB.
4. Urządzenie posiada zasoby sprzętowe pozwalające przełączać 19 Mpps oraz 20 Gbps ruchu.
5. Urządzenie domyślnie pozwala na przełączanie z prędkością 2,5 Gbps i umożliwia licencyjne odblokowanie wydajności do następujących wartości: 5 Gbps, 10 Gbps, 20 Gbps.
6. Urządzenie posiada dedykowany akcelerator kryptograficzny osiągający wydajność 5 Gbps dla ruchu IMIX.
7. Urządzenie posiada minimum 8 GB pamięci RAM.
8. Urządzenie obsługuje 1 000 000 prefiksów w tablicach ruting IPv4.
9. Urządzenie obsługuje 1 000 000 prefiksów w tablicach ruting IPv6.
10. Urządzenie obsługuje 100 000 tras multicast.
11. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP.
12. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP.
13. Urządzenie obsługuje Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter) z możliwością definiowania polityk per aplikacja.
14. Urządzenie umożliwia uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routingu Forwarding), umożliwiając m.in. wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci.
15. Urządzenie obsługuje 8000 instancji wirtualnych tablic routingu.
16. Urządzenie obsługuje funkcjonalność Bidirectional Forwarding Detection (BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego.
17. Urządzenie obsługuje funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF.
18. Urządzenie obsługuje multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN.
19. Urządzenie obsługuje protokół NHRP (ang. Next Hop Resolution Protocol).
20. Urządzenie obsługuje protokół GDOI (RFC 3547).
21. Funkcjonalności związane z niezawodnością pracy:

a. system modularny umożliwiający aktualizację poszczególnych modułów programowych niezależnie od siebie
b. redundancja procesów rutingowych realizowana poprzez uruchomienie dwóch kopii systemu operacyjnego
c. BFD dla OSPF, BGP, ISIS
d. IP FRR
e. BGP Prefix-Independent Convergence (PIC)
f. Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP
g. funkcjonalność VRRP
h. redundantne zasilacze 230V
i. możliwość wymiany modułów w trakcie pracy (ang. hot swap)

22. Urządzenie obsługuje MPLS, w szczególności:
a. LDP
b. EoMPLS, VPLS
c. MPLS L3 VPN
d. MPLS TE
e. MPLS FRR w trybach protekcji łącza oraz węzła

23. Urządzenie obsługuje następujące mechanizmy jakości usług (QoS):
a. klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN zarówno dla IPv4 jak i IPv6
b. hierarchiczny QoS (H-QoS) - 3 poziomy
c. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP.
d. dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek
e. algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek
f. możliwość obsługi jednej kolejki z priorytetem w stosunku do innych
g. mechanizm ograniczania ilości ruchu w kolejce priorytetowej
h. możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
i. możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting)
j. mechanizm WRED
k. możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS

24. Urządzenie obsługuje następujące funkcje i elementy bezpieczeństwa:
a. sprzętowa ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu
b. Unicast RPF (Reverse Path Forwarding)
c. listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL
d. 30 000 wpisów IPv4 na wszystkich listach kontroli dostępu (ACL), a także 4 000 list kontroli dostępu (ACL)
e. dostęp administracyjny oparty o role z przypisanymi uprawnieniami
f. zasoby sprzętowe umożliwiające uruchomienie funkcjonalności zapory ogniowej typu statefull (ang. statefull firewall) poprzez dodanie odpowiedniej licencji, przy czym zapora ogniowa:
    i. umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi

strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji)
ii. obsługuje ruch IPv4 oraz IPv6
iii. umożliwia konfigurację polityk per wirtualna tablica routingu (VRF)
iv. umożliwia obsługę 2 000 000 równoczesnych sesji
v. umożliwia zestawianie 200 000 nowych połączeń HTTP na sekundę

g. zasoby sprzętowe realizujące funkcjonalności szyfrowania VPN z wydajnością 5 Gbps (AES256) z obsługą 8 000 tuneli Spiec
h. sieci VPN typu site-2-site oparte o Spiec
i. dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP w relacji spoke to spoke w celu optymalizacji transmsji danych pomiędzy oddziałami
j. bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast
k. algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), w szczególności:
    i. Elliptic Curve Diffie-Hellman (ECDH)
    ii. Galois Counter Mode Advanced Encryption Standard (GCM-AES) - 128/256 bitów
    iii. Galois Message Authentication Code (GMAC-AES) - 128/256 bitów
    iv. Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2
l. konfiguracja tuneli IPSec VPN w oparciu o protokół IKEv2
    i. IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych
    ii. IKEv2 zarówno dla ruchu IPv4 jak i IPv6
m. funkcjonalność VPN per VRF
n. ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU
o. logowanie pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU
p. możliwość uruchomienia funkcjonalności analizy i klasyfikacji pakietów w warstwie 2-7 polegającej na przeszukiwaniu pakietów pod kątem zawierania specyficznych ciągów znaków i wykrywania na tej podstawie ataków

25. Urządzenie umożliwia uruchomienie usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów, przy czym klasyfikacja ta:
    a. opiera się na kilku mechanizmach gwarantujących poprawne rozpoznawanie wielu aplikacji / protokołów
    b. udostępnia 3 atrybuty opisujące daną aplikację / protokół (atrybuty ułatwiają konfigurowanie QoS na urządzeniu poprzez grupowanie podobnych aplikacji / protokołów - na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji).
    c. nie wymaga rozbudowy sprzętowej urządzenia, jedynie zakup licencji
26. Urządzenie obsługuje 4000 tuneli GRE.
27. Urządzenie posiada możliwość tunelowania przesyłanych danych w postaci tuneli GRE typu punkt-punkt oraz punkt-wielopunkt z możliwością uruchomienia protokołów routingu dynamicznego pomiędzy urządzeniami połączonymi za pomocą tuneli GRE.
28. Urządzenie umożliwia ochronę kryptograficzną tuneli GRE.
29. W ramach funkcjonalności zarządzania, urządzenie:
    a. umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3
    b. obsługuje Ethernet OAM (IEEE 802.3ah, IEEE 802.1ag, ITU-T Y.1731)
    c. obsługuje MPLS OAM

d. umożliwia pisanie skryptów konfiguracyjnych
e. obsługuje protokół Netflow ze wsparciem dla multicast oraz IPv4/IPv6
f. posiada narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP
g. posiada obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+
h. posiada dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet 10/100/1000 oraz port AUX
i. posiada port USB
j. posiada możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej
    i. konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona
k. urządzenie posiada możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów

30. Urządzenie posiada redundantne zasilacze AC 230V zintegrowane w obudowie urządzenia.
31. Urządzenie umożliwia montaż w szafie 19".
32. Urządzenie musi być dostarczone z czterema portami obsadzonymi modułami 1000Base-T

6.3. Urządzenie pełniące funkcję ściany ogniowej i bramy VPN – 8 szt.

Wykonawca ma obowiązek dostarczyć sprzęt nie gorszy niż wyspecyfikowany poniżej (w tabeli):

Symbol	Opis	Ilość
ASA5525-FPWR-K9	ASA 5525-X with FirePOWER Services, 8GE, AC, 3DES/AES, SSD	1
CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	1
SF-ASA-X-9.2.2-K8	ASA 9.2.2 Software image for ASA 5500-X Series,5585-X,ASA-SM	1
SF-ASA-FP5.4-K9	Cisco FirePOWER Software v5.4 for ASA 5500-X	1
ASA5525-CTRL-LIC	Cisco ASA5525 Control License	1
ASA-IC-B-BLANK	ASA 5525-X Interface Card Blank Slot Cover	1
ASA5500X-SSD120INC	ASA 5512-X through 5555-X 120GB MLC SED SSD (Incl.)	1
ASA5525-MB	ASA 5525 IPS Part Number with which PCB Serial is associated	1
ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	1
L-ASA5525-TA=	Cisco ASA5525 FirePOWER IPS License	1
L-ASA5525-TA-3Y	Cisco ASA5525 FirePOWER IPS 3YR Subscription	1

Wymagania minimalne w przypadku zaproponowania urządzeń równoważnych:

Architektura urządzenia:

1. Urządzenie o konstrukcji modularnej pełniące funkcję bramy VPN i ściany ogniowej (firewall) typu Statefull Inspection. Urządzenie musi mieć możliwość dalszej rozbudowy sprzętowej.

2. Urządzenie wyposażone w:
    a. osiem interfejsów Gigabit Ethernet 10/100/1000 (RJ45)
    b. dedykowany interfejs Gigabit Ethernet 10/100/1000 (RJ45) do zarządzania
3. Urządzenie obsługuje interfejsy VLAN-IEEE 802.1q na interfejsach fizycznych (200 sumarycznie).
4. Urządzenie wyposażone w moduł sprzętowego wsparcia szyfrowania 3DES i AES oraz licencje na szyfrowanie 3DES/AES.
5. Urządzenie posiada dedykowany dla zarządzania port konsoli.
6. Urządzenie posiada pamięć Flash o pojemności umożliwiającej przechowanie, co najmniej 3 obrazów systemu operacyjnego i 3 plików konfiguracyjnych.
7. Urządzenie posiada pamięć DRAM o pojemności 8GB, umożliwiającej uruchomienie wszystkich dostępnych dla urządzenia funkcjonalności.
8. Urządzenie zapewnia możliwość klastrowania dla zwiększania wydajności pomiędzy dwoma odległymi fizycznie ośrodkami. Wspierane są dwa urządzenia w klastrze.

Zasilanie urządzenia

9. Urządzenie posiada zasilacz umożliwiający zasilanie prądem przemiennym 230V.

Wydajność urządzenia

10. Przepustowość stanowego firewall'a wynosi 2 Gbps, a dla ruchu rzeczywistego (tzw. ruch multiprotocol) 1 Gbps.
11. Urządzenie posiada wydajność 300 Mbps dla ruchu szyfrowanego protokołami 3DES, AES.
12. Urządzenie umożliwia terminowanie 750 jednoczesnych sesji VPN (IPSec VPN, SSL VPN).
13. Urządzenie zapewnia zestawianie do 750 tuneli SSL VPN w trybie client-based i clientless VPN.
14. Urządzenie obsługuje 500000 jednoczesnych sesji/połączeń z prędkością zestawiania 20000 połączeń na sekundę. Dla pakietów 64 bajtowych urządzenie posiada wydajność 700000 pakietów na sekundę.
15. Urządzenie posiada możliwość agregacji interfejsów fizycznych (IEEE 802.3ad) – 4 łączy zagregowanych. Pojedyncze łącze zagregowane może składać się z 2 interfejsów.
16. Urządzenie obsługuje funkcjonalność Access Control List (ACL) – zarówno dla ruchu wchodzącego, jak i wychodzącego. Minimalna obsługiwana ilość reguł 200000 linii.
17. Obsługa 200 VLAN'ów.

Funkcjonalność urządzenia:

18. Urządzenie pełni funkcję ściany ogniowej śledzącej stan połączeń (tzw. Stateful Inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji.
19. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (tzw. Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory.
20. Urządzenie posiada możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos.
21. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
22. Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access).

23. Urządzenie zapewnia w zakresie SSL VPN weryfikację uprawnień stacji do zestawiania sesji, poprzez weryfikację następujących cech:
    a. OS Check - system operacyjny
    b. IP Address Check - adres z jakiego następuje połączenie
    c. File Check - pliki w systemie
    d. Registry Check - wpisy w rejestrze systemu Windows
    e. Certificate Check - zainstalowane certyfikaty
24. Urządzenie posiada, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym, klienta VPN dla technologii IPSec VPN i SSL VPN.
25. Oprogramowanie klienta VPN (IPSec oraz SSL) ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows (7, XP – wersje 32 i 64-bitowe) i Linux i umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC.
26. Oprogramowanie klienta VPN obsługuje protokoły szyfrowania 3DES/AES.
27. Oprogramowanie klienta VPN umożliwia blokowanie lokalnego dostępu do Internetu podczas aktywnego połączenia klientem VPN (wyłączanie tzw. split-tunnelingu).
28. Urządzenie ma możliwość pracy, jako transparentna ściana ogniowa warstwy drugiej modelu ISO OSI.
29. Urządzenie obsługuje protokół NTP.
30. Urządzenie współpracuje z serwerami CA.
31. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego. Urządzenie wspiera translację adresów (NAT) dla ruchu multicastowego.
32. Urządzenie zapewnia mechanizmy redundancji, w tym:
    a. możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby, active/active dla kontekstów
    b. umożliwia pracę w klastrze
33. Urządzenie realizuje synchronizację tablicy połączeń pomiędzy węzłami pracującymi w trybie wysokiej dostępności HA.
34. Urządzenie zapewnia możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia.
35. Urządzenie zapewnia funkcjonalność stateful failover dla ruchu VPN.
36. Urządzenie posiada mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:
    a. Hypertext Transfer Protocol (HTTP),
    b. File Transfer Protocol (FTP),
    c. Extended Simple Mail Transfer Protocol (ESMTP),
    d. Domain Name System (DNS),
    e. Simple Network Management Protocol v 1/2/3 (SNMP),
    f. Internet Control Message Protocol (ICMP),
    g. SQL*Net,
    h. inspekcji protokołów dla ruchu voice/video – H.323 (włącznie z H.239), SIP, MGCP, RTSP
37. Urządzenie umożliwia zaawansowaną normalizację ruchu TCP:
    a. poprawność pola TCP ACK
    b. poprawność sekwencjonowania segmentów TCP
    c. poprawność ustanawiania sesji TCP z danymi
    d. limitowanie czasu oczekiwania na segmenty nie w kolejności
    e. poprawność pola MSS
    f. poprawność pola długości TCP
    g. poprawność skali okna segmentów TCP non-SYN

h. poprawność wielkości okna TCP

38. Urządzenie ma możliwość blokowania aplikacji (np. peer-to-peer, czy „internetowy komunikator") wykorzystujących port 80.
39. Urządzenie zapewnia obsługę i kontrolę protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługi komend wprowadzonych wraz z protokołem ESMTP.
40. Urządzenie ma możliwość inspekcji protokołów HTTP oraz FTP na portach innych niż standardowe.
41. Urządzenie zapewnia wsparcie stosu protokołów IPv6, w tym:
    a. listy kontroli dostępu dla IPv6
    b. możliwości filtrowania ruchu IPv6 na bazie nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload
    c. inspekcję protokołu IPv6, pracując w trybie transparentnym
    d. adresację IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover)
    e. realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6
42. Urządzenie obsługuje mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu.
43. Urządzenie umożliwia współpracę z serwerami autoryzacji w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik.
44. Urządzenie obsługuje routing statyczny i dynamiczny (min. dla protokołów RIP, OSPF i BGP).
45. Urządzenie pozwala na osiągnięcie wysokiej dostępności dla protokołów routingu dynamicznego, tzn. trasy dynamiczne zawarte w tablicy routingu są synchronizowane z urządzenia active na urządzenie standby.
46. Urządzenie umożliwia zbieranie informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL).
47. Urządzenie umożliwia konfigurację globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie.
48. Urządzenie umożliwia konfigurację reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu.
49. Urządzenie umożliwia pominięcie stanu sesji TCP w scenariuszach wdrożeniowych z asymetrycznym przepływem ruchu.
50. Urządzenie wspiera Proxy dla protokołu SCEP i umożliwia zautomatyzowany proces pozyskiwania certyfikatów przez użytkowników zdalnych dla dostępu VPN.
51. Urządzenie wspiera użytkownika korzystającego z trybu klienta VPN (IPSec oraz SSL) oraz clientless SSL VPN, w zakresie obsługi haseł w systemie Microsoft AD, bezpośrednio lub poprzez ACS, dla obsługi sytuacji wygaśnięcia terminu ważności hasła w systemie Microsoft AD, umożliwiając zmianę przeterminowanego hasła.
52. Urządzenie obsługuje IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode. Ponadto urządzenie wspiera protokół IKEv2 (Internet Key Exchange w wersji 2) dla połączeń zdalnego dostępu VPN oraz site-to-site VPN opartych o protokół IPSec.
53. Urządzenie umożliwia rozbudowę poprzez zakup odpowiedniej licencji lub oprogramowania bez konieczności dokonywania zmian sprzętowych, w tym istnieje możliwość wirtualizacji konfiguracji poprzez wirtualne konteksty. Urządzenie wspiera maksymalnie 20 wirtualnych kontekstów.

Funkcjonalność urządzenia – NGFW

54. Urządzenie zapewnia funkcjonalności tzw. Next-Generation Firewall w następującym zakresie:
    a. system automatycznego wykrywania i klasyfikacji aplikacji (tzw. Application Visibility and Control)
    b. system IPS
    c. system filtrowania ruchu w oparciu o URL
    d. system ochrony przed malware
55. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System tworzy konteksty z wykorzystaniem poniższych parametrów:
    a. wiedza o użytkownikach – uwierzytelnienie
    b. wiedza o urządzeniach – pasywne skanowanie ruchu
    c. wiedza o urządzeniach mobilnych
    d. wiedza o aplikacjach wykorzystywanych po stronie klienta
    e. wiedza o podatnościach
    f. wiedza o bieżących zagrożeniach
    g. baza danych URL
56. System posiada otwarte API dla współpracy z systemami zewnętrznymi, takimi jak SIEM.
57. System automatycznego wykrywania i klasyfikacji aplikacji (AVC):
    a. posiada możliwość klasyfikacji ruchu i wykrywania 3000 aplikacji sieciowych
    b. zapewnia wydajność 375 Mbps
    c. pozwala na tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług
    d. pozwala na wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
    e. umożliwia współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach
58. System IPS:
    a. zapewnia skuteczność wykrywania zagrożeń i ataków na poziomie 95%, udokumentowaną przez niezależnie testy
    b. posiada możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)
    c. posiada możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu)
    d. posiada możliwość wykrywania i eliminowania szerokiej gamy zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługę VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, zagrożenia dnia zerowego, itp.)
    e. posiada możliwość wykrywania modyfikacji znanych ataków, jak i tych nowo powstałych, które nie zostały jeszcze dogłębnie opisane
    f. zapewnia następujące sposoby wykrywania zagrożeń:
        i. sygnatury ataków opartych na exploitach,
        ii. reguły oparte na zagrożeniach,
        iii. mechanizm wykrywania anomalii w protokołach

iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego

g. posiada możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego, włącznie z możliwością sprawdzania zawartości pakietu
h. posiada mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives)
i. posiada możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń
j. posiada wiele możliwości reakcji na zdarzenia, takich jak monitorowanie, blokowanie ruchu zawierającego zagrożenia, zastępowanie zawartość pakietów oraz zapisywanie pakietów
k. posiada możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
l. posiada możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności (systemy operacyjne, serwisy, otwarte porty, aplikacje oraz zagrożenia) w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności
m. posiada możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych
n. zapewnia możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
o. posiada możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
p. zapewnia możliwość obrony przed atakami skonstruowanymi tak, aby uniknąć wykrycia przez IPS - w tym celu stosuje odpowiedni mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego
q. zapewnia mechanizm bezpiecznej aktualizacji sygnatur - zestawy sygnatur/reguł pobierane są z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
r. zapewnia możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie
s. jest zarządzany poprzez system centralnego zarządzania za pomocą szyfrowanego połączenia
t. zapewnia obsługę reguł Snort
u. zapewnia możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS
v. zapewnia mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (tzw. Indication of Compromise)
w. zapewnia mechanizmy automatyzacji w zakresie dostrojenia polityk bezpieczeństwa
x. posiadać możliwość wykorzystania mechanizmów obsługi ruchu asymetrycznego firewall'a dla uzyskania pełnej widoczności ruchu – w szczególności posiada możliwość pracy w trybie HA firewalla oraz w trybie klastrowania
y. pozwala na pracę z przepustowością 255 Mbps przy jednoczesnym działaniu AVC

59. System filtrowania ruchu w oparciu o URL:
    a. pozwala na kategoryzację stron w 70 kategoriach
    b. zapewnia bazę URL o wielkości 250 mln URL
60. System ochrony przed malware:
    a. zapewnia sprawdzenie reputacji plików w systemie globalnym
    b. zapewnia sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze)
    c. zapewnia narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych później jako oprogramowanie złośliwe (analiza retrospektywna)
    d. zapewnia wykrywanie ataków typu Zero-Day
61. System zapewnia centralną konsolę zarządzania zapewniającą informacje ogólne i szczegółowe o:
    a. wykrytych hostach
    b. aplikacjach
    c. zagrożeniach i atakach
    d. wskazaniach kompromitacji (tzw. Indication of Compromise) na podstawie:
        i. zdarzeń z IPS
        ii. malware backdoors
        iii. exploit kits
        iv. ataków na aplikacje webowe
        v. połączeń do serwerów Command'n'Control
        vi. wskazań eskalacji uprawnień
    e. zdarzeń sieciowych
        i. połączeń do znanych adresów IP Command'n'Control
    f. zdarzeń związanych z malware
        i. wykrytego malware
        ii. wykrytej infekcji dropperów

Zarządzanie i konfiguracja

62. Urządzenie posiada możliwość eksportu informacji przez syslog.
63. Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub analogicznego.
64. Urządzenie posiada możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS i TACACS+ oraz obsługuje mechanizmy AAA (Authentication, Authorization, Accounting).
65. Urządzenie jest konfigurowalne przez CLI oraz interfejs graficzny.
66. Dostęp do urządzenia jest możliwy przez SSH.
67. Urządzenie obsługuje protokół SNMP v 1/2/3.
68. Możliwa jest edycja pliku konfiguracyjnego urządzenia w trybie off-line. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją.
69. Urządzenie umożliwia zrzucenie obecnego stanu programu (tzw. coredump) dla potrzeb diagnostycznych.
70. Urządzenie posiada wsparcie dla mechanizmu TCP Ping, który pozwala na wysyłanie wiadomości TCP dla rozwiązywania problemów związanych z łącznością w sieciach IP.
71. Urządzenie umożliwia kontrolę dostępu administracyjnego za pomocą protokołu TACACS+.

Obudowa i licencjonowanie

72. Urządzenie ma możliwość instalacji w szafie typu rack 19".
73. Wysokość urządzenia wynosi 1RU.
74. urządzenie musi być dostarczone z 3-letnią subskrypcją na IPS, jednocześnie musi umożliwiać rozbudowę o dodatkowe funkcjonalności w zakresie filtrowania URL jak i ochrony przed malware.

6.4. System zarządzania urządzeniami pełniącymi funkcję ściany ogniowej i bramy VPN – 1 szt

Wykonawca ma obowiązek dostarczyć rozwiązanie nie gorsze niż wyspecyfikowane poniżej (w tabeli):

Symbol	Opis	Ilość
FS-VMW-10-SW-K9	Cisco Firepower Management Center,(VMWare) for 10 devices	1

W przypadku zaproponowania rozwiązania równoważnego, system do administrowania i zarządzania funkcjami NGFW musi spełniać następujące wymagania minimalne:

1. System musi zostać dostarczony w formie maszyny wirtualnej wraz z odpowiednią platformą sprzętową oraz niezbędnymi licencjami do wirtualizacji
2. System musi zapewniać:
    a. centralne zarządzanie urządzeniami, licencjami, zdarzeniami i politykami bezpieczeństwa w Centrali oraz we wszystkich Oddziałach,
    b. separację uprawnień administracyjnych z wykorzystaniem funkcjonalności typu RBAC/role-based management,
    c. możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i zdalnie,
    d. możliwość spersonalizowania widoków i raportów dostarczanych przez system do wymagań Zamawiającego,
    e. agregację wszystkich zdarzeń bezpieczeństwa oraz centralne monitorowanie i analizę działając w czasie rzeczywistym oraz korelację wielu zdarzeń i wykorzystanie skorelowanej wiedzy do zapobiegania zagrożeniom,
    f. tworzenie całościowych raportów dotyczących sytuacji w sieci oraz raportów sprofilowanych pod kątem określonego zdarzenia,
    g. konfigurację automatycznego pobierania zestawów sygnatur na najnowsze zagrożenia i podatności; system musi mieć możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami,
    h. funkcjonalność typu harmonogram zadań umożliwiając automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityk IPS,
    i. dogłębne wykorzystanie informacji kontekstowych (takich jak informacje o konfiguracji, zachowaniu sieci i hostów) w celu poprawienia efektywności i dokładności procesu manualnej i automatycznej analizy incydentów,
    j. możliwość dynamicznego dostrajania systemu IPS przy zachowaniu minimalnej interwencji administratora poprzez selekcję reguł, zmianę konfiguracji i uaktualnienia polityk,
    k. gromadzenie logów ze wszystkich obsługiwanych sond IPS,

l. przechowywanie incydentów, logów oraz innych informacji generowanych przez system zarówno w wewnętrznej bazie danych jak i możliwość udostępniania do zabezpieczonego wglądu w te informacje zewnętrznym aplikacjom w trybie tyko do odczytu,
m. zaawansowany system przeszukiwania logów powalający na przeprowadzanie analizy:
    i. aktualnego stanu danego urządzenia,
    ii. podglądu historii dostępnych zasobów,
    iii. możliwość eliminacji powtarzających się alarmów (tzw. Black Listing),
n. tworzenie wielu polityk bezpieczeństwa zawierających różne zestawy sygnatur i przydzielania ich do segmentów zdefiniowanych na różnych urządzeniach
o. możliwość co najmniej dwóch rodzajów implementacji polityki bezpieczeństwa:
    i. wysłanie polityki tylko do przypisanego urządzenia,
    ii. wysłanie polityki do każdego z dostępnych urządzeń;
p. reguły wykrywania zagrożeń muszą mieć możliwość modyfikacji i rozszerzenia,
q. reguły wykrywania zagrożeń muszą być oparte na ogólnodostępnym języku składni tak, aby użytkownicy mogli tworzyć je samodzielnie jak i edytować te dostarczane przez producenta systemu,
r. możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu,
s. funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia poprzez odpowiedzi, aż do rozwiązania,
t. możliwość automatycznej odpowiedzi na zagrożenia przez:
    i. alarmy,
    ii. rekonfigurację zapory ogniowej,
    iii. rekonfigurację routingu,
u. tworzenie profilu ruchu sieciowego w normalnych warunkach (profil podstawowy) wykorzystując różne technologie analizy przepływów (np. NetFlow) i możliwość wykrycia odchylenia od profilu podstawowego; funkcjonalność ta musi przedstawiać sposób wykorzystania pasma sieciowego w celu ułatwienia wykrywania przeciążeń i przestojów urządzeń sieciowych,
v. przegląd wszystkich zdarzeń związanych z bezpieczeństwem pod kątem analizy powłamaniowej i wczesnej prewencji włamań,
w. możliwości integrowania się z rozwiązaniami firm trzecich typu Vulnerability Scanner/Vulnerability Management, dostarczających dodatkowych informacji na temat luk i podatności istniejących w monitorowanych środowiskach w celu bardziej precyzyjnego szacowania skutków zagrożeń oraz automatycznego procesu strojenia polityki bezpieczeństwa,
x. za pośrednictwem otwartego API możliwość integracji z innymi systemami typu SIEM, systemami obsługi zgłoszeń itp.,
y. usługi dynamicznej reputacji znanych adresów IP propagujących zagrożenia w sieci Internetowej oraz możliwość definiowania własnych, zewnętrznych źródeł informacji; adresy te powinny byś blokowane jako znane zagrożenia i kategoryzowane według typu stwarzanego zagrożenia,
z. w ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie musi mieć możliwość interaktywnego blokowania z resetowaniem zapytań; w ramach tej funkcji musi zostać zapewniona możliwość zdefiniowania własnej

strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia.

3. System musi zapewniać obsługę zdalnych uaktualnień, wykonywania kopii zapasowych oraz przywracania jak i funkcjonalność odinstalowywania uaktualnień bez konieczności fizycznego dostępu do urządzenia.
4. Całość komunikacji pomiędzy poszczególnymi komponentami systemu musi byś zabezpieczona protokołem kryptograficznym.
5. System musi zapewnić możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP.
6. Reguły wykrywające nowo ujawnione zagrożenia i luki muszą być wygenerowane przez dostawcę w przeciągu 48 godzin od ich ogłoszenia.
7. System musi byś dostępny przez interfejs Web, bez potrzeby instalacji dodatkowego oprogramowania klienckiego.
8. System musi zapewnić przechowywanie do 10 milionów zdarzeń IPS.
9. System musi zapewnić możliwość zarządzania co najmniej dziesięcioma urządzeniami.

Zamawiający zarządza aktualnie użytkowanymi urządzeniami ASA z funkcjonalnością FirePower za pomocą oprogramowania Cisco Firepower Management Center. W ramach rozbudowy, wymaga się dostarczenia licencji i wdrożenia drugiej instancji oprogramowania do zarządzania systemem firewall. Istniejąca instancja systemu będzie musiała być zrekonfigurowana na potrzeby zarządzania częścią dostarczonych w niniejszym postępowaniu urządzeń firewall. Pozostałe urządzenia będą zarządzane przy pomocy opisanego powyżej systemu zakupionego w niniejszym postępowaniu. Zamawiający dopuszcza jego zainstalowanie na urządzeniach dostarczanych zgodnie z punktem 6.7.

6.5. System telemetrii sieciowej, wykrywania zagrożeń i ataków – 1 kpl.

Wykonawca ma obowiązek dostarczyć rozwiązanie nie gorsze niż wyspecyfikowane poniżej (w tabeli):

Symbol	Opis	Ilość
L-LC-SMC-VE-K9	StealthWatch Management Console Virtual Edition	1
L-LC-FC-NF-VE-K9	StealthWatch FlowCollector for NetFlow Virtual Edition	1
L-LC-FC-SF-VE-K9	StealthWatch FlowCollector for sFlow Virtual Edition	1
L-LC-FPS-10K=	StealthWatch flow collection license for 10,000 flows/sec	1

Wymagania minimalne w przypadku zaproponowania rozwiązania równoważnego:

Wymagania ogólne

System telemetrii sieciowej w sieci Zamawiającego przewidziany jest jako narzędzie wspomagające zarządzanie siecią LAN/WAN oraz systemami bezpieczeństwa. Celem jego zastosowania jest pozyskanie dodatkowych informacji sieci w tym dokładnych danych dla systemów zarządzania oraz systemów wykrywających ataki i nadużycia w sieci.

System analizy danych telemetrycznych przewidziany jest do diagnozowania niepożądanych incydentów w sieci, wykrywania anomalii ruchowych oraz błędów konfiguracyjnych. Dla zastosowań związanych bezpieczeństwem system powinien zapewniać mechanizmy związane z wykrywaniem ataków, zagrożeń i wskazywać anomalie. System musi wykorzystywać telemetrię z urządzeń LAN/WAN i pozwalać na pobieranie szczegółowych danych z urządzeń sieciowych Zamawiającego.

System analizy telemetrii musi działać w oparciu o heurystykę i nie może być budowany wyłącznie w oparciu o sygnaturowe wykrywanie nadużyć. W założeniu

Zamawiającego system musi posiadać możliwość pobrania i analizy informacji sieciowych raportowanych z wykorzystaniem protokołu NetFlow (RFC 3954) – co najmniej w odniesieniu do posiadanych urządzeń sieciowych przez Zamawiającego i/lub protokołów równoważnych jeżeli takowe są wymagane/wspierane jednocześnie przez producenta urządzeń sieci WAN oraz systemu telemetrii sieciowej.

Architektura systemu

1. System musi obejmować całościowo narzędzia pozwalające na pozyskanie i analizę zdarzeń i incydentów zachodzących w siecie w szczególności system powinien obejmować
    a. Centralną konsolę zarządzania – wszystkie zdarzenia powinny być możliwe do wyświetlenia i analizy przez centralną konsolę
    b. Narzędzie (kolektor) zbierania informacji o przepływach danych – NetFlow Collector
    c. Narzędzie generowania informacji o przepływach danych z segmentów sieciowych, z których pobranie informacji natywnie z infrastruktury sieciowej nie jest możliwe. Rozwiązanie musi posiadać możliwość pozyskania takiej informacji co najmniej z:
        i. przełączników sieciowych LAN pozwalających na przesyłanie kopii ruchu na wskazany port (SPAN port)
        ii. środowiska zwirtualizowanego – wymagane co najmniej wsparcie środowiska Vmware z VMotion
    d. Narzędzie zapewniające informację o tożsamości użytkownika integrujące się co najmniej z Active Directory, LDAP, serwerami haseł jednorazowych OTP i serwerami CA
2. System musi wykorzystywać jako dane źródłowe niepróbkowany (non-sampled) eksport NetFlow przesyłanie co najmniej przez NetFlow v5, NetFlow v9
3. System musi umożliwiać wykorzystanie danych źródłowych w formie próbkowanej (sampled) z użyciem protokołu sFlow lub odpowiednika
4. System operacyjny rozwiązania musi być co najmniej wzmocnionych systemem operacyjnym (optymalnie dedykowanym systemem operacyjnym) z ograniczoną liczbą otwartych portów
5. System musi posiadać możliwość pracy w modelu redundantnym w szczególności musi być możliwość redundancji kolektorów eksportów Netflow oraz centralnej konsoli zarządzania.
6. System musi być przygotowany do obsługi 10 000 flow na sekundę oraz umożliwiać rozbudowę do 30 000 flow na sekundę poprzez doposażenie (niedopuszczalna jest wymiana komponentów). System musi umożliwiać rozbudowę poprzez zwiększenie liczby kolektorów NetFlow oraz sFlow, w zależności od wybranego protokołu.

Wykrywanie ataków/anomalii

7. System musi zapewniać behawioralne metody wykrywania ataków/anomalii
8. System musi umożliwiać profilowanie ruchu poszczególnych hostów i grup hostów poprzez długotrwałą (co najmniej 20 dni) ciągłą obserwację jego zachowań - celem wykrywania anomalii/ataków wynikających z
    a. przekroczenia wartości bazowych (zarówno zdefiniowanych przez administratora jak i wynikających z „uczenia się" systemu charakterystyk ruchowych) dla typowego wzorca ruchu dla stacji,
    b. zmiany charakterystyki ruchu dla stacji
    c. naruszenia założonej polityki bezpieczeństwa

9. System musi umożliwiać wykrywanie ataków Zero-Day
10. System musi umożliwiać wskazanie zarażonych hostów wewnątrz organizacji
11. System musi umożliwiać wskazanie ataków, które zostały dopuszczone przez ominięcie systemów AV
12. System musi umożliwiać wykrywanie ataków polimorficznych, mutujących jak też zaszyfrowanych w oparciu o zmiany zachowania w sieci atakowanego hosta
13. System musi posiadać wbudowane mechanizmy algorytmy korelowania zdarzeń celem wyświetlenia administratorowi zagregowanych zdarzeń o największym potencjalnym zagrożeniu
14. System musi umożliwiać wykrywania ataków DoS i DDoS wraz ze wskazaniem celu ataku jak też hostów atakujących
15. System musi posiadać możliwość różnicowania zachowań hostów w zależności od pory dnia i dnia tygodnia co najmniej dla:
    a. Statystki ruchowej hosta
    b. Całościowego ruchu generowanego przez hosta
    c. Wolumenu ruchu pakietów z flagą SYN
    d. Maksymalnego poziomu ruchu pakietów z flagą SYN
16. System musi uwzględniać zmiany wynikające z typowych działań i rozwoju organizacji i posiadać zdolność „uczenia się" – przykładowo uwzględniać zmiany charakterystyki ruchu serwera, który w przeciągu roku zwiększył wolumen ruchu kilkakrotnie i odpowiednio do niego dostosowywać odpowiednie wartości progowe.
17. System musi raportować o wyciekach danych
    a. Z hostów wewnętrznych na zewnątrz organizacji
    b. Z serwerów – na jeden lub więcej hostów wewnątrz organizacji
    c. Z hosta wewnętrznego w formie rozsiania na większą liczbę hostów wewnątrz organizacji
18. System musi umożliwiać konfigurację „soft-firewalla" w sieci celem raportowania o niepożądanych przepływach ruchu pomiędzy wskazanymi obszarami sieci.
19. System musi posiadać możliwość raportowania w przypadku naruszenia polityki zdefiniowanej przez administratora. Raport dla administratora musi zawierać co najmniej informację
    a. o rodzaju komunikacji, która naruszyła politykę,
    b. ile razy polityka została naruszona
    c. wskazanie użytkownika, który dokonał tego naruszenia wraz z podaniem jego adresu IP
20. System musi posiadać możliwość pobrania „z chmury" informacji reputacyjnej o hostach zewnętrznych (system musi posiadać możliwość rozbudowy o wskazaną funkcję – nie jest ona wymagana w systemie stanowiącym przedmiot zamówienia)
21. System musi posiadać możliwość pobierania informacji z „chmury" o serwerach Botnet Command and Control (system musi posiadać możliwość rozbudowy o wskazaną funkcję – nie jest ona wymagana w systemie stanowiącym przedmiot zamówienia)
22. System musi posiadać mechanizmy wykrywania sytuacji usuwania danych ze wskazanych serwerów (np. serwerów plików) przez atakującego z wewnątrz jak i z zewnątrz sieci
23. System musi umożliwiać wykrywanie zagrożeń z wykorzystaniem geolokacji – w szczególności
    a. Raportować o połączeniach VPN z uwzględnieniem kraju, z którego nawiązane jest połączenie

b. Informować o „podwójnym" logowaniu się użytkowników z oddalonych od siebie lokalizacji

Narzędzia monitorowania sieci

24. System musi posiadać możliwość wykrywania źle skonfigurowanych lub niepoprawnie funkcjonujących urządzeń sieciowych i hostów w tym routerów, serwerów i stacji roboczych
25. System musi posiadać możliwość monitoringu interfejsów sieciowych monitorowanych urządzeń w tym interfejsów agregowanych
26. System musi zapewniać możliwość monitoring wykorzystania interfejsu z dokładnością do usługi sieciowej
27. System musi zapewniać możliwość raportowania wykorzystania interfejsów i usług sieciowych z granulacją nie mniejszą niż 1 minuta
28. System musi posiadać możliwość wskazania „TopX" hostów i usług dla wskazanego połączenia sieciowego
29. System musi posiadać możliwość definiowania aplikacji i ich automatycznej identyfikacji z dokładnością do poziomu Skype, Teredo, AIM, WebEx, Dropbox, Facebook itp..
30. System musi posiadać wbudowane narzędzia rozpoznawania co najmniej 900 aplikacji.
31. System musi posiadać możliwość definiowania raportów z wykorzystaniem informacji o własnych definicjach aplikacji przygotowanych przez administratora
32. System musi posiadać możliwość raportowania nieaktywności/aktywności poszczególnych hostów
33. System musi posiadać możliwość definiowania raportów analitycznych dla wolumenów ruchu
34. System musi
    a. posiadać wbudowane narzędzia zaawansowanej deduplikacji informacji o przepływach (flow),
    b. zapewniać unikalność flow i nie powielać informacji o pojedynczym flow w raportach.
35. Pojedynczy przepływ danych musi być identyfikowany raz i pokazywany w raportach jako jeden strumień danych bez względu na ścieżkę danych.
36. System musi uwzględniać, iż na ścieżce przesyłu danych będą posiadane przez Zamawiającego następujące urządzenia sieciowe opisane w punkcie 4, oraz poniższe:
    a. Routery Cisco serii ASR 3800, 3900
    b. Switche Cisco Nexus 7k oraz Catalist 6800
    c. Switche Catalyst 6500 (wraz z zainstalowanym modułem ACE30)
    d. Switche Juniper EX
    e. Firewalle Juniper SRX
    f. Firewalle CheckPoint
    g. Firewalle sieciowe Cisco ASA
37. System musi posiadać możliwość wskazania hostów, na których uruchomiona jest określona usługa lub uruchomiony klient aplikacji
38. System musi posiadać możliwość wskazania „wykorzystania" określonych portów TCP/UDP
39. System musi zapewniać mechanizmy „trendingu" dla sieci i ruchu, w szczególności dla:
    a. całkowitego wolumenu ruchu,
    b. oddzielnie dla ruchu wyjściowego i wejściowego,

c. ilości nowych/starych/nieaktywnych hostów,
d. ilości flow

40. System musi umożliwiać raportowanie z wykorzystaniem Differentiated Services jako atrybutu
41. System musi umożliwiać raportowanie z wykorzystaniem ASN jako atrybutu
42. System musi umożliwiać monitorowanie sieci korzystających z IPv6 oraz sieci ze środowiskiem mieszanym IPv4/IPv6
43. System musi zapewniać możliwość monitorowania parametrów
    a. RTT – round trip time
    b. SRT – Server response time
    c. Retransmisji w sieci
44. System musi posiadać możliwość wykrywania rekonesansu w sieci w tym wykonywanie skanowania po portach
45. System musi posiadać możliwość alarmowania w przypadku skanowania sieci i kierowania ruchu do nieaktywnych hostów
46. System musi umożliwiać monitorowanie maszyn wirtualnych (co najmniej pracujących w środowisku VMWare) w tym raportowanie ruchu odbywającego się w ramach środowiska wirtualnego i wychodzącego ze środowiska wirtualnego (system musi posiadać możliwość rozbudowy o wskazaną funkcję – nie jest ona wymagana w systemie stanowiącym przedmiot zamówienia)
47. System musi posiadać wbudowany mechanizm mapowania host-to-host
48. System musi posiadać możliwość raportowania nadużycia zasobów organizacji np.
    a. Ponadnormatywne korzystania z internetu
    b. Korzystanie z portali społecznościowych
    c. Dostęp do systemów „wrażliwych"
    d. Wykorzystanie protokołów lub aplikacji które nie zostały dopuszczone do użytku w sieci
49. System musi posiadać możliwość raportowania o pojawieniu się w sieci nowej niedopuszczonej przez administratora aplikacji
50. System musi posiadać możliwość raportowania informacji o hostach próbujących ominąć (bypass) serwery proxy
51. System musi posiadać wbudowaną analitykę pozwalajacą na wykrywanie wycieków danych (Data Leak) co najmniej z wykorzystaniem telemetrii dla wolumenu ruchu i telemetrii dotyczącej czasu połączenia do sieci zewnętrznych.

Analiza i przechowywanie informacji o flow

52. System nie powinien wymagać modelu FPC (Full Packet Capture) do działania i analizy. Rozwiązanie powinno działać w oparciu o analizę Netflow. W przypadku gdy Oferent zakłada zastosowanie rozwiązania FPC system musi być odpowiednio wyskalowany aby obsłużyć całościowy ruch Zamawiającego.
53. System musi zapewniać możliwość przechowywania exportów Netflow i informacji o flow przez co najmniej 180 dni z wszystkimi szczegółami dotyczącymi flow. Poszczególne flow muszą być opisane co najmniej 80 atrybutami
54. System musi posiadać narzędzia graficznego przedstawiania przepływów (flow) w sieci.
55. System musi umożliwiać graficzne kreślenie propagacji malware w sieci
56. System musi posiadać możliwość analizy flow pod kątem wykrywania ruchu P2P takiego jak KaZaa, Gnutella, eDonkey itp.

57. System musi posiadać możliwość pasywnego rozpoznawania systemów operacyjnych używanych przez użytkowników (passive fingerprinting). Wymagane jest wykrywanie co najmniej 60 systemów operacyjnych.

Zarządzanie

58. System zarządzający musi wspierać połączenia bezpiecznym kanałem szyfrowanym z wykorzystaniem SSL
59. System musi posiadać możliwość ograniczenia dostępu do stacji zarządzającej do pojedynczych hostów lub też do grupy hostów
60. System musi posiadać możliwość uwierzytelnienia z wykorzystaniem zewnętrznych serwerów RADIUS i TACACS+
61. System musi umożliwiać różnicowanie dostępu dla administratorów, w szczególności musi pozwalać na
    a. Ograniczenie grup hostów, które może monitorować dany administrator
    b. Ograniczenie czynności które może wykonać dany administrator
    c. Ograniczenie dostępu tylko do odczytu – read-only
    d. Ograniczenie informacji,do których ma dostęp dany administrator np.
        i. Administrator1 ma dostęp do statystyk urządzeń sieciowych, charakterystyk ruchu i innych danych dotyczących monitoringu sieciowego
        ii. Administrator2 ma dostęp do informacji o naruszeniu polityk, outbreak i innych danych dotyczących bezpieczeństwa
62. System musi umożliwiać predefiniowanie raportów, które będą generowane cyklicznie we wskazanym przez administratora reżimie czasowym
63. System musi umożliwiać tworzenie raportów z wykorzystaniem geolokacji – w szczególności raportów per kraj

Współpraca i integracja z systemami zewnętrznymi

64. System musi zapewniać możliwość integracji z systemami zewnętrznymi co najmniej z wykorzystaniem SOAP i API (producenta systemu)
65. Wszystkie logi, wykresy oraz raporty muszą być eksportowalne do zewnętrznych plików, odpowiednio w formacie CSV, JPG (lub równoważny format graficzny) i PDF
66. System powinien zapewniać raportowanie o zdarzeniach i incydentach co najmniej przez Syslog, SNMP i Email,
67. System musi zapewniać możliwość integracji z zewnętrznymi systemami klasy SIEM
68. System musi posiadać możliwość współpracy z zewnętrznymi systemami co najmniej z wykorzystaniem SNMP i syslog
69. System musi posiadać możliwość współpracy z zewnętrznymi systemami firewall i zapewniać mechanizm „łączenia flow" po przejściu przez NAT.
70. System musi posiadać możliwość współpracy i pobierania danych do analizy z zewnętrznych systemów IDS/IPS z wykorzystaniem sygnatur opisywanych w języku SNORT
71. System musi posiadać możliwość współpracy i pobierania danych z zewnętrznych systemów Firewall wysyłających wiadomości syslog
72. System musi posiadać możliwość współpracy z usługami katalogowymi takimi jak ActiveDirectory
73. System musi zapewniać możliwość współpracy i integracji z systemami uwierzytelnienia pracujących z użyciem protokołu 802.1x takim jak system Cisco ISE (Identity Services Engine) lub podobny w zakresie
    a. RADIUS proxy

b. Przenoszenie informacji o tożsamości użytkowników uwierzytelnionych przez serwer 802.1x
c. Przenoszenie informacji o profilu hosta po profilowaniu dokonanym przez serwer 802.1x
d. Przenoszenie informacji o kontekście użytkownika przechowywanym przez serwer 802.1x

74. System nie może wymagać instalacji jakiegokolwiek oprogramowania (agenta/klienta) na stacjach końcowych celem pobierania informacji z hostów.
75. System musi posiadać możliwość współpracy z urządzeniami sieciowymi co najmniej w zakresie obsługi skryptów TCL i pozwalać na reagowanie na ataki co najmniej poprzez przepisanie listy kontroli dostępu (ACL), wstrzyknięcie „NullRoute" i blokowanie portów. Opcje blokowania powinny obejmować co najmniej
    a. blokowanie ruchu z określonego źródła
    b. blokowanie ruchu do określonego celu
    c. blokowanie portu
    d. blokowanie usługi

Zakres dostawy

76. Dostarczony system musi obejmować:
    a. Kolektor NetFlow – 1 sztuka, kolektor sFlow – 1 sztuka oraz Centralna konsola zarządzająca – 1sztuka, a także wszelkie licencje gwarantujące obsługę 10 000 przepływów (flow)
    b. Rozwiązanie musi być dostarczone z subskrypcją dla w/w funkcji na co najmniej 3 lata
    c. System może zostać dostarczony w jednej z dwóch postaci:

<u>Wariant A.</u>

1) Dedykowane rozwiązanie (appliance) dla wszystkich komponentów o parametrach poniżej:
    a. Kolektory dla eksportów NetFlow i sFlow w postaci dedykowanego urządzenia o następujących parametrach
        i. Obsługa do 25000 flows na sekundę
        ii. Obsługa do 500 eksporterów Netflow
        iii. Obsługa najmniej 1 TB przestrzeni dyskowej dla przechowywania danych (w przypadku dedykowanego urządzenia pamięć musi być redundantna w RAID-6 lub lepszym)
        iv. Co najmniej 3 interfejsy dla zbierania eksportów Netflow - 1Gbps
        v. Co najmniej 1 interfejs zarządzający 1Gbps (10/100/1000)
2) Centralną konsolę zarządzania w postaci dedykowanego urządzenia o następujących parametrach
    a. Obsługa do 5 kolektorów danych zapewniających pobieranie danych telemetrycznych dla 50 000 flow na sekundę
    b. Obsługa najmniej 1 TB przestrzeni dyskowej dla przechowywania danych (redundantna w RAID-6 lub lepszej)
    c. Co najmniej 1 interfejs zarządzający 1Gbps (10/100/1000) (dotyczy dedykowanego urządzenia)

<u>Wariant B.</u>

Maszyny wirtualne na serwerach Zamawiającego będących przedmiotem niniejszego postępowania (opisane w punkcie 6.7). W przypadku dostarczenia konsoli zarządzania i oprogramowania kolektorów z postaci maszyny wirtualnej Zamawiający dopuszcza możliwość wykorzystania serwerów będących przedmiotem niniejszego postępowania o ile spełniają one parametry rekomendowane przez Producenta Kolektorów NetFlow/sFlow oraz centralnej konsoli zarządzającej. Oferent zobowiązany wówczas także do dostarczenia wszystkich innych niezbędnych dla uruchomienia rozwiązania elementów programowych np. oprogramowanie wirtualizatora.

6.6. System uwierzytelnienia dostępu do sieci LAN/WLAN/VPN – 1 kpl.

Wykonawca ma obowiązek dostarczyć rozwiązanie nie gorsze niż wyspecyfikowane poniżej (w tabeli):

Symbol	Opis	Ilość
Systemu kontroli dostępu do sieci w oparciu o tożsamość użytkownika		
L-ISE-BSE-500=	Cisco Identity Services Engine 500 EndPoint Base License	1
L-ISE-PLS-S-500=	Cisco ISE 500 Endpoint Plus Subscription License	1
L-ISE-APX-S-500=	Cisco ISE 500 Endpoint Apex Subscription License	1
L-ISE-TACACS=	Cisco ISE Device Admin License	1
AC-APX-3YR-500-S	Cisco AnyConnect 3-Yr 500 User Apex License	1
L-AC-APX-S-3Y-500	Cisco AnyConnect 3-Yr 500 User Apex (ASA License Key)	1
AC-APX-3YR-500	Cisco AnyConnect 3-Yr 500 User Apex Subscription	1
Platformy dla systemu kontroli dostępu		
SNS-3515-K9	Small Secure NetWork Server for ISE Applications	2
SW-3515-ISE-K9	Cisco **ISE** Software forthe SNS-3515-K9 appliance	1
CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	1
UCSC-PSU1-770W=	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	2
ISE-VM-K9=	Cisco Identity Services Engine Virtual Machine Image	2

Wymagania minimalne w przypadku zaproponowania rozwiązania równoważnego:

Podstawowe cechy systemu

1. System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.
2. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.
3. System musi umożliwiać obsługę co najmniej 500 urządzeń końcowych dołączonych do sieci oraz zapewniać skalowalność do przynajmniej 7500 urządzeń poprzez rozbudowę istniejącego wdrożenia.
4. System musi umożliwiać przeprowadzenie głębokiej analizy systemu co najmniej 500 urządzeń końcowych dołączonych do sieci.
5. System musi umożliwiać instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym:
    a. Na hypervisorze VMWare ESXi co najmniej 5.x
    b. Na serwerach fizycznych wspieranych przez producenta
6. System musi umożliwiać wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym:

a. Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji systemu oraz jego monitorowanie
b. Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:
    i. przełączników dostępowych
    ii. sesji uwierzytelniania 802.1 X
    iii. zdarzeń kontroli dostępu (autoryzacji)
    iv. zdarzeń związanych z błędami
    v. zdarzeń związanych z alarmami systemowymi
c. Wydzielenie serwerów usługowych realizujących funkcje:
    i. serwera RADIUS oraz TACACS dla infrastruktury sieciowej
    ii. serwera polityk uwierzytelniania i kontroli dostępu 802.1X
    iii. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego
    iv. serwera profilowania stacji końcowych
d. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, w tym:
    i. zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu oraz systemu monitoringu
e. System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych - co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS
f. System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
g. System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
h. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
i. System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System musi wymuszać hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni
j. System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
    i. dostęp do interfejsu konfiguracji usług tożsamości 802.1X
    ii. dostęp do interfejsu konfiguracji urządzeń sieciowych
    iii. dostęp do interfejsu konfiguracji polityk
    iv. dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
    v. dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
k. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.

Mechanizmy uwierzytelniania 802.1x

7. System musi wspierać następujące protokoły uwierzytelniania i standardy:
    a. RADIUS, zgodnie z dokumentami:
        i. RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
        ii. RFC 2139 — RADIUS Accounting

iii. RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
iv. RFC 2866 — RADIUS Accounting
v. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
vi. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
vii. RFC 2869 — RADIUS Extensions

b. RADIUS Proxy dla zewnętrznego serwera RADIUS

8. System musi wspierać protokół Windows Active Directory, w tym co najmniej następujące repozytoria AD:
   a. Microsoft Windows Active Directory 2003 32bit
   b. Microsoft Windows Active Directory 2003 R2 32bit i 64bit
   c. Microsoft Windows Active Directory 2008 32bit i 64bit
   d. Microsoft Windows Active Directory 2008 R2 64bit
   e. Microsoft Windows Active Directory 2012
   f. Microsoft Windows Active Directory 2012 R2
9. System musi wspierać protokół Lightweight Directory Access Protocol (LDAP)
10. System musi wspierać serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865
11. System musi wspierać następujące protokoły uwierzytelniania:
    a. PAP/ASCII
    b. CHAP
    c. MS-CHAPv1
    d. MS-CHAPv2
    e. EAP-MD5
    f. LEAP
    g. EAP-TLS
12. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
    a. EAP-MS-C HAPv2
    b. EAP-GTC
    c. EAP-TLS
13. System musi umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect
14. System musi wspierać implementację 802.1X z przynajmniej następującymi suplikantami:
    a. wbudowanym klientem 802.1X dla Windows 7
    b. wbudowanym klientem 802 1X dla Windows 8 i 8.1
    c. wbudowanym klientem 802.1x dla Windows 10
    d. Apple Mac OS X Supplicant
    e. Apple iOS Supplicant
    f. Google Android Supplicant
15. System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based).
16. System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.
17. System musi umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o złożone reguły.
18. System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)
19. System musi posiadać lokalną bazę stacji końcowych. Lokalna baza stacji końcowych musi być tworzona per stacja końcowa na podstawie unikalnego adresu MAC.

20. System musi wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC
21. System musi wspierać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - NetWork Access Devices), w tym:
    a. tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port
    b. tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia
    c. tryb uwierzytelniania 802.1X, w którym dozwolone jest jedno urządzenie telefonii IP w domenie głosowej (Voice VLAN) i jeden host w domenie danych (Data VLAN) na jednym porcie fizycznym
    d. tryb uwierzytelniania 802.1X zezwalający na wiele hostów na jednym porcie fizycznym
    e. mechanizm umożliwiający poprawną obsługę sytuacji, w której nowy host podłącza się do portu, na którym uprzednio było uwierzytelnione urządzenie, w tym w VLANie głosowym
    f. mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X
    g. mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACl) w procesie uwierzytelnienia i kontroli dostępu 802.1X
    h. obsługa przypisania listy kontroli dostępu dla przekierowania ruchu Web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki
    i. mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych
    j. mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny
    k. przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników
    l. uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego się w VLANie głosowym
    m. współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN
    n. możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web o możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika
22. System musi wspierać uwierzytelnianie nazwą użytkownika i hasłem przez portal Web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X)
23. System wspiera przynajmniej następujące urządzenia sieciowe, jako klientów RADIUS (NAD - NetWork Access Device):
    a. Przełączniki Ethernet dostarczane w ramach projektu Zamawiający wymaga potwierdzenia (wskazania w dokumentacji producenta systemu uwierzytelnienia) wsparcia dla proponowanych platform LAN ze wskazaniem wspieranych wersji oprogramowania

Realizacja dostępu gościnnego

24. System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym co najmniej dla:
    a. Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7 (co najmniej Microsoft Edge, MS IE, Mozilla Firefox, Google Chrome)
    b. Apple Mac OS X 10.x (Safari, Mozilla Firefox Google Chrome)
    c. Apple iOS 9.x, 8.x, 7.x, 6.x 5.x (Safari)
    d. Google Android dla 2.2 i nowszych (Native Browser i Mozilla Firefox)
    e. Linux (Mozilla Firefox, Google Chrome)
25. System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby (administrator).
26. System musi zapewniać uwierzytelnienie administratora, które musi odbywać się sekwencyjnie w oparciu o:
    a. wewnętrzną bazę użytkowników
    b. zewnętrzne repozytorium użytkowników
27. System musi umożliwiać konfigurację uprawnień administratora, w tym uprawnienia do:
    a. logowania się do systemu
    b. tworzenia pojedynczego konta gościnnego
    c. tworzenia wielu kont gościnnych
    d. importowania kont gościnnych z pliku CSV
    e. wysyłania wiadomości email po utworzeniu konta gościnnego
    f. wysyłania wiadomości SMS po utworzeniu konta gościnnego
    g. wyświetlenia hasła konta gościnnego
    h. wydrukowania danych konta gościnnego
    i. wyświetlenia danych stworzonych kont gościnnych
    j. zawieszenia (suspend) i reinicjacji kont gościnnych
28. System musi umożliwiać personalizację wyglądu portalu administratora i gościa, w tym:
    a. zmianę logo strony logowania
    b. zmianę obrazu tła strony logowania
    c. zmianę logo bannera
    d. zmianę obrazu tła bannera
    e. zmianę koloru tła strony z treścią
29. System musi umożliwiać zmianę konfiguracji portów portalu administratora, gościa i administratora, w tym portu HTTPS
30. System musi umożliwiać zmianę adresu URL i FQDN strony administratora.
31. System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie. System musi umożliwiać wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych
32. System musi posiadać wbudowane, wspierane przez producenta wzorce językowe dla stron administratora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim
33. System musi umożliwiać stworzenie własnego wzorca językowego dla stron administratora i gościa, w tym w języku polskim.
34. System musi umożliwiać wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez administratora:
    a. Imienia

b. Nazwiska
c. Firmy
d. adresu e-mail
e. numeru telefonu
f. danych opcjonalnych (nie mniej niż 5 dodatkowych pól)

35. System musi umożliwiać konfigurację dla użytkowników gościnnych:
    a. wyświetlenia im informacji polityce akceptowalnego użycia sieci (AUP)
    b. zezwolenia gościom na zmianę hasła
    c. samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez administratora
36. System musi umożliwiać honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.
37. System musi umożliwiać konfigurację maksymalnej ilości nieudanych logować do konta gościnnego.
38. System musi umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługiwać co najmniej 20 urządzeń per konto gościnne.
39. System musi umożliwiać konfigurację czasu ważności hasła w dniach.
40. System musi umożliwiać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny.
41. System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych
42. System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego, w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika
43. System musi umożliwiać tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu.
44. System musi umożliwiać przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.
45. System musi umożliwiać udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP i poprzez SMS,
46. System musi wspierać API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.

Profilowanie urządzeń

47. System musi umożliwiać dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
48. System musi umożliwiać wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności musi zapewniać stworzenie polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc.
49. System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:
    a. DHCP
    b. DHCP SPAN
    c. HTTP
    d. RADIUS
    e. DNS
    f. SNMP
    g. NetWork Scan (NMAP lub inne narzędzie profilowania aktywnego)

50. System musi umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.
51. System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
52. System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:
    a. Stacji roboczych pracujących z systemami FreeBSD, Linux, Macintosh, Microsoft Windows, Sun,
    b. Urządzeń mobilnych: Android, Apple, Blackberry
    c. Telefonów IP
    d. Drukarek sieciowych
    e. Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych
    f. Routerów
    g. Punktów dostępu bezprzewodowego
53. System musi umożliwiać zarówno subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, jak również **umożliwiać wgrywania aktualizacji manualnie za pomocą zewnętrznych nośników danych,** w tym następujących informacji:
    a. reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci
    b. reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt
54. System musi umożliwiać włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie.
55. System musi wspierać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta lub zainstalowanych manualnie za pomocą zewnętrznych nośników danych.

Głęboka analiza stacji końcowej (Posture Assessment)

56. System musi umożliwiać badanie stanu bezpieczeństwa stacji klienckich
57. Musi umożliwiać:
    a. Badanie czy stacja ma zainstalowane określone oprogramowanie (np. system antywirusowy, czy ma aktualne sygnatury, itp.)
    b. Badanie czy istnieją określone pliki na dysku
    c. Badanie określonych wpisów w rejestrach
    d. Badanie czy jest uruchomiony określony proces
    e. Badanie czy jest włączona określona usługa
58. W przypadku stwierdzenia niezgodności z polityką musi być możliwość przełączenia stacji do środowiska, w którym może nastąpić remediacja (np. przełączenie do VLANu, w którym będzie możliwe np. pobranie poprawek antywirusowych)

Współdzielenie kontekstu z innymi systemami

59. System musi wspierać dedykowane API, dla współdzielenia informacji kontekstowej z innymi systemami producenta i systemami innych producentów.
60. Informacja kontekstowa obejmuje przynajmniej nazwę uwierzytelnionego przez system użytkownika i adres IP jego stacji końcowej

Administracja urządzeniami

61. System musi umożliwiać, w oparciu o protokół TACACS, określanie czy użytkownik/administrator posiada prawo dostępu do urządzeń sieciowych oraz umożliwiać nadanie użytkownikowi odpowiednich praw dostępowych w celu administracji. Wymagane jest uruchomienie funkcjonalności we wdrażanym rozwiązaniu.

Obsługa serwerów certyfikatów CA.

62. System musi posiadać funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.
63. Funkcja CA musi umożliwiać wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS.
64. System musi wspierać hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów.
65. Funkcja CA musi zapewniać przynajmniej następujące funkcjonalności:
    a. Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS
    b. Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym
    c. Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji
    d. Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA

Raportowanie

System musi umożliwiać generowanie przynajmniej następujących raportów:

66. raportów dla protokołów AAA:
    a. diagnostyki protokołów AAA
    b. trendów uwierzytelnienia 802.1X
    c. accountingu RADIUS
    d. uwierzytelniania RADIUS
    e. raportów dozwolonych protokołów
67. sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:
    a. uwierzytelnień pomyślnych
    b. uwierzytelnień nieudanych
68. „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:
    a. uwierzytelnień pomyślnych
    b. uwierzytelnień nieudanych
69. raportów dla poszczególnych instancji serwerów systemu, w tym:
    a. uwierzytelnień RADIUS per serwer
    b. Top „N"uwierzytelnień per serwer
    c. monitorowania Online Certificate Status Protocol (OCSP)
    d. administratorów systemu i ich uprawnień
    e. logowania administratorów do systemu
    f. zmian konfiguracji serwera dokonanych przez administratorów
    g. stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
    h. zmian operacyjnych serwera dokonanych przez administratorów

i. zmian haseł przez użytkowników

70. raportów dla stacji końcowych, w tym:
    a. uwierzytelnień typu MAC Authentication
    b. Top „N" uwierzytelnień per adres MAC stacji
    c. Top „N" uwierzytelnień per maszyna
    d. Top „N"uwierzytelnień per RADIUS Calling Station ID
    e. działań podsystemu profilera per adres MAC
    f. czasu wymaganego na sprofilowanie stacji per adres MAC
71. raportów dla błędów, w tym:
    a. błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
    b. sumarycznych przyczyn nieudanych uwierzytelnień
    c. Top „N" uwierzytelnień per rodzaj błędu
72. raportów dla urządzeń sieciowych:
    a. sumarycznych uwierzytelnień dla urządzeń sieciowych
    b. Top „N" uwierzytelnień per urządzenie sieciowe
    c. niedostępności serwera AAA dla urządzenia sieciowego
    d. wiadomości logowanych przez urządzenia sieciowe
    e. stanu portów i sesji urządzenia sieciowego widocznych przez SNMP
    f. raportów użytkowników:
        i. sumarycznych uwierzytelnień użytkowników
        ii. Top „N"uwierzytelnień per użytkownik
        iii. sesji użytkowników gościnnych
        iv. aktywności użytkowników gościnnych
        v. sumarycznych uwierzytelnień administratorów dostępu gościnnego
        vi. uwierzytelnień per unikalny użytkownik
73. raportów katalogu sesji
    a. aktywnych sesji RADIUS
    b. historii sesji RADIUS
    c. zaterminowanych sesji RADIUS

Alarmy

74. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą
    a. wiadomości e-mail
    b. syslog
75. Alarmy muszą być generowane w następujących sytuacjach:
    a. ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu
    b. opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego
    c. status krytycznych procesów będzie niepożądany, w tym status:
        i. procesu wewnętrznej bazy danych systemu
        ii. serwera aplikacyjnego systemu
        iii. bazy danych sesji
        iv. kolektora i procesora wiadomości log
        v. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej)
        vi. stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:
            1. obciążenie systemu (load)
            2. zajętość pamięci
76. System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:

a. badanie łączności IP za pomocą ping, nslookup, traceroute
b. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
    i. nazwy użytkownika
    ii. adresu MAC
    iii. statusu uwierzytelnienia (udana lub nieudana)
    iv. powodu, jeżeli uwierzytelnienie nieudane
    v. zakresu czasowego, co do dnia, godziny i minuty
c. wykonanie zdalnego polecenia na urządzeniu sieciowym
d. ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
    i. definicji serwerów AAA
    ii. protokołu RADIUS
    iii. odkrywania urządzeń
    iv. logowania
    v. uwierzytelniania Web
    vi. konfiguracji trybu 802.1X
e. wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu

Dopuszczalne sposoby realizacji rozwiązania

Zamawiający wymaga spełnienia następujących warunków realizacji systemu uwierzytelnienia dostępu do sieci:

77. Zamawiający wymaga użycia dedykowanego rozwiązania sprzętowego w celu realizacji polityk autentykacji, autoryzacji, accountingu, profilingu, administracji urządzeniami oraz przeprowadzenia procesu analizy stacji końcowej.
78. Zamawiający wymaga redundancji rozwiązań w celu zapewnienia wysokiej dostępności działania usług.
79. Zamawiający wymaga uruchomienia usług współdzielących kontekst z innymi systemami w formie dedykowanego urządzenia fizycznego lub maszyny wirtualnej, z założeniem spełnienia wymogów niezawodności oraz redundancji rozwiązania.
80. Zamawiający dopuszcza stosowanie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów.
81. W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców Zamawiający oczekuje, iż system będzie zapewniał pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN/WLAN/APN. Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia)
82. W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców Zamawiający oczekuje iż system będzie serwisowany przez jednego producenta tzn. zgłoszenia serwisowe będą kierowane do jednego dostawcy Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia).
83. W przypadku zastosowania serwera CA jako dedykowanego rozwiązania Zamawiający będzie traktował to rozwiązanie jako integralną część systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia)
84. Zamawiający wymaga poświadczenia ze strony producenta systemu uwierzytelnienia pełnego wsparcia dla platform dostarczanych w ramach postępowania w szczególności obejmuje to:
    a. Przełączniki Ethernet dostarczane w ramach projektu. Zamawiający wymaga potwierdzenia (wskazania w dokumentacji producenta systemu

uwierzytelnienia) wsparcia dla proponowanych platform LAN ze wskazaniem wspieranych wersji oprogramowania

b. Poświadczenie takie nie jest wymagane jeżeli taka współpraca opisana jest w oficjalnej dokumentacji producenta (jako wspierane rozwiązanie, należy wówczas przedłożyć dokumentację) lub w przypadku gdy poszczególne rozwiązania pochodzą od tego samego producenta.

85. Zamawiający wymaga dostarczenia rozwiązania dla co najmniej 500 użytkowników w zakresie funkcjonalności bazowej i co najmniej dla 500 w zakresie funkcjonalności rozszerzonej (profilowanie).
86. Zamawiający wymaga dostarczenia rozwiązania w zakresie głębokiej analizy stacji końcowej (Posture Assessment) dla co najmniej 500 użytkowników
87. Zamawiający dopuszcza użycie licencji udzielonych przez producenta w ramach wyposażenia innych urządzeń dostarczanych w niniejszym postępowaniu.
88. Rozwiązanie musi być dostarczone z subskrypcją dla w/w funkcji na co najmniej 3 lata
89. W przypadku konieczności zastosowania na stacjach końcowych dodatkowego suplikanta lub innych modułów wymaganych do spełnienia zakładanych funkcjonalności Zamawiający wymaga dostarczenia odpowiednich licencji wraz z odpowiednią subskrypcją na co najmniej 3 lata

Platforma dla systemu kontroli dostępu

90. Rozwiązanie musi być wspierane platformą dla systemu kontroli dostępu do sieci w oparciu o tożsamość użytkownika opisanego powyżej. Zarówno platforma jak i oprogramowanie musi być wspierana przez serwis producenta.
91. Obudowa musi pozwalać na instalację w RACK 19“ i musi być dostarczona wraz z zestawem do zamontowania serwerów w szafie teleinformatycznej 19", umożliwiającym pełne wysunięcie obudowy o wysokości nie przekraczającej 1U.
92. Musi mieć zainstalowany procesor Intel serii E5 posiadający co najmniej 6 rdzeni, taktowany zegarem co najmniej 2.4GHz
93. Musi mieć zainstalowaną pamięć RAM - co najmniej 16GB
94. Musi posiadać co najmniej jeden dysk 2.5 cala, 10K RPM, SAS o pojemności co najmniej 600GB
95. Musi posiadać co najmniej 4 interfejsy Gigabit Ethernet
96. Płyta główna musi posiadać/spełniać warunki:
    a. musi być zaprojektowana przez producenta serwera i oznaczona trwale jego logo
    b. dwa fizyczne gniazda do obsługi procesorów wyspecyfikowanych w następnych punktach
    c. sloty do obsługi pamięci ECC DDR-4 lub nowszych
    d. możliwość wyposażenia serwera w 512GB RAM
    e. musi mieć możliwość instalacji kontrolera macierzy SAS 12Gbps umożliwiający obsługę minimum 5-miu dysków w konfiguracjach RAID 0/1/10 ze wsparciem dla Vmware
    f. musi mieć wbudowany Software Raid (6Gbps) ze wsparciem co najmniej 8 dysków SATA (RAID 0,1,10)
    g. Zintegrowana karta graficzna
    h. Co najmniej 2 sloty PCI-Express 3-ciej generacji, oba wyprowadzone na zewnątrz serwera, w tym min. 1 dla karty pełnej wysokości, połowy długości z konektorem minimum x16. Jeśli do obsługi slotów PCIe niezbędne

są dodatkowe komponenty mechaniczne należy dostarczyć je razem z serwerem

i. Wewnętrzny slot USB 2.0 umieszczony na płycie głównej serwera, umożliwiający bootowanie
j. Wbudowany podwójny slot kart SD (wymagana certyfikacja z vmware 5.5 do startu systemu)

97. Płyta musi obsługiwać procesory spełniające następujące wymagania
    a. Procesor o architekturze 64bitowej
    b. Liczba obsługiwanych kanałów pamięci 4 per CPU
    c. wbudowane w procesor wsparcie dla obsługi standardu PCIe 3.0
    d. zintegrowany kontroler zarządzania pamięcią
    e. Maksymalna moc wydzielanego ciepła 135W
    f. Zaoferowany procesor musi wspierać funkcjonalność dynamicznego i automatycznego zwiększenia wydajności serwera dla aplikacji poprzez zwiększenie częstotliwości rdzenia
98. Musi być wyposażony w chipset dedykowany przez producenta procesora do pracy w konfiguracjach 2 procesorowych, obsługujący opisane procesory
99. Musi posiadać moduł KVM wyprowadzony na przedni panel serwera pozwalający uzyskać dostęp do gniazda monitora, 2xUSB oraz portu szeregowego. Jeżeli w celu wykorzystania funkcjonalności niezbędny jest dodatkowy moduł, należy dostarczyć go razem z serwerem
100. Serwer musi umożliwiać instalację w sumie minimum 8-iu dysków twardych 2,5" bez konieczności wymiany komponentów rozwiązania.
101. Serwer musi umożliwiać instalację następujących systemów operacyjnych: Microsoft Windows Server 2012 R2 w wersji Standard i Enterprise, VMWare vSphere w wersji Advanced , Enterprise, Enterprise Plus.
102. Wszystkie komponenty rozwiązania muszą znajdować się na oficjalnej liście wsparcia HCL danego serwera
103. Musi być wyposażony w co najmniej 2 porty VGA (1 przy wykorzystaniu interfejsu kvm na przednim panelu i 1 z tyłu obudowy serwera)
104. Musi posiadać co najmniej 1 port RS232
105. Musi posiadać co najmniej 1 port RJ-45 10/100/1000 dedykowany dla zarządzania.

Zarządzanie:

106. Serwer musi mieć moduł zdalnego zarządzania (w tym zdalnej konsoli), który pozwala na:
    a. zdalne włączenie, wyłączenie i restart serwera,
    b. wykorzystanie zdalnej, graficznej konsoli obsługującej zdalną pracę na serwerze
    c. podgląd logów sprzętowych serwera,
    d. przejęcie pełnej konsoli graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS)
    e. podłączanie wirtualnych napędów CD i FDD oraz obrazów
    f. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w slocie PCI.
    g. Konfiguracje kontrolera SCSI (grupy RAID itp)
    h. Konfiguracje parametrów BIOS (takie jak kolejność bootowania, wirtualizacja kart PCIe)
107. Serwer musi mieć możliwość zarządzania poprzez centralną platformę producenta serwerów z jednego miejsca. Platforma musi umożliwiać:

a. Inwentaryzację sprzętu (w tym automatyczne detekcje serwerów i ich rejestracje w systemie)
b. Monitorowanie stanu serwerów
c. Zarządzanie serwerem - centralny IP KVM
d. Zarządzanie firmware komponentów (zdalny upgrade)
e. Automatyczne zgłaszanie błędów/awarii do producenta sprzętu
f. Zarządzanie mocą (power capping)
g. Dostęp (w tym IP KVM i funkcje zarządzania/monitorowania) oparte o role (RBAC)

Zasilanie, chłodzenie

108. Musi być wyposażony w co najmniej dwa zasilacze wymienne podczas pracy serwera
109. Musi posiadać redundantne chłodzenie serwera/CPU, minimum 5 wentylatorów

Inne wymagania

110. Musi zostać dostarczony z preinstalowanym systemem kontroli dostępu do sieci w oparciu o tożsamość użytkownika.

6.7. Środowisko serwerowe na potrzeby systemów zarządzania – 1 kpl.

W przypadku zaoferowania sprzętu równoważnego do opisanego poniżej zamawiający wymaga prawidłowej współpracy między wszystkimi komponentami opisanego w niniejszym punkcie środowiska.

6.7.1. Oprogramowanie do backupu

Wykonawca ma obowiązek dostarczyć rozwiązanie nie gorsze niż wyspecyfikowane poniżej (w tabeli):

P-VBRENT-VS-P0000-00	Veeam Backup & Replication Enterprise for VMware - Public Sector	20
P73-07041	Windows Svr Std 2016 64Bit English DVD 5 Clt	2

Wymagania minimalne w przypadku zaproponowania rozwiązania równoważnego:

Wymagania ogólne

1. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 oraz Microsoft Hyper-V 2012 i 2012 R2. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
2. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
3. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V

Całkowite koszty posiadania

5. Oprogramowanie musi być licencjonowanie w modelu "per-CPU". Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji.

Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone

6. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
7. Oprogramowanie musi tworzyć "samowystarczalne" archiwa, do odzyskania których nie jest wymagana osobna baza danych z metadanymi deduplikowanych bloków
8. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
9. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.
10. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
11. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
12. Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
13. Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość akutalizacji pola „notatki" na wirtualnej maszynie
14. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.
15. Oprogramowanie musi oferować portal samoobłsugowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL (w tym odtwarzanie point-in-time)
16. Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 5.1, 5.5, 5.6 i 8.0 i archiwizować również metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD
17. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
18. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
19. Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza
20. Oprogramowanie musi wspierać backup maszyn wirtualych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
21. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO (Recovery Point Objective)

22. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej

23. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak, aby nie były przekraczane skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
24. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
25. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
26. Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server
27. Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
28. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
29. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku gdy repozytorium backupów jest umiejscowione na EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
30. Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku gdy repozytorium backupów jest umiejscowione na HP StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
31. Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
32. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
33. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
34. Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
35. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
36. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
37. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

Wymagania RTO (Recovery Time Object)

38. Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla srodowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania
39. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jezeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować jaką migrację swoimi mechanizmami
40. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
41. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej

maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

42. Oprogramowanie musi mieć możliwość odtworzenia plików przy pomocy VMware VIX API
43. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
    a) **Linux**
        i) ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs
    b) **BSD**
        i) UFS, UFS2
    c) **Solaris**
        i) ZFS
    d) **Mac**
        i) HFS, HFS+
    e) **Windows**
        i) NTFS, FAT, FAT32, ReFS
44. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
45. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
46. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.
47. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
48. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
49. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
50. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
51. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
52. Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
53. Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
54. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

55. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
56. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem

57. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere

System operacyjny

58. System powinien być dostarczony wraz z systemem operacyjnym.

6.7.1.1. Pamięć masowa do przechowywania backupu

Wykonawca ma obowiązek dostarczyć sprzęt nie gorszy niż wyspecyfikowany poniżej (w tabeli):

Part Number	Produkt	Ilość
PC-EUROPE-1	POWER CORD,DD EUROPE CONT,CEE7/7,C13,2M	2
C-10GMCU2P	OPTION,DD 10GBE,IO MODULE,CU SFP,2PORT	1
DD2200	SYSTEM DD2200 NFS CIFS	1
DD2200-24TB	SYSTEM DD2200-12X2HDD SAS 24TB NFS CIFS	1
C-FLDIN2200	OPTION FIELD INSTALL KIT DD2200	1
M-PREHWDD-E1	PREMIUM SYSTEM SUPPORT (DD)	1
L-RLC-2200	LICENSE RETENTION LOCK COMPL DD2200=IA	1
M-PRESWDD-E1	PREMIUM SOFTWARE SUPPORT (DD)	1
L-REP-2200	LICENSE REPLICATOR DD2200=IA	1
M-PRESWDD-E1	PREMIUM SOFTWARE SUPPORT (DD)	1
L-BST-2200	LICENSE BOOST DD2200=IA	1
M-PRESWDD-E1	PREMIUM SOFTWARE SUPPORT (DD)	1
L-DDOE-DD2200-24	LICENSE BASE DD OE DD2200-24=IA	1
M-PRESWDD-E1	PREMIUM SOFTWARE SUPPORT (DD)	1
L-XCAP2200-B	LICENSE EXPSTOR DD2200=IA	1
M-PRESWDD-E1	PREMIUM SOFTWARE SUPPORT (DD)	1
DDOS-DOC-A4N	DOCS,DD OS DOC,A4	1

Wymagania minimalne w przypadku zaproponowania rozwiązania równoważnego:

1. Przedmiotem zamówienia jest dostarczenie urządzenia do de-duplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.
2. Oferowane urządzenie musi posiadać minimum
   a) 4 porty Ethernet 1 Gb (wymagane w urządzeniu) i możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, BOOST, OST
   b) 2 porty Ethernet 10 Gb i możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, de-duplikacja na źródle
3. Oferowane urządzenie musi mieć możliwość (przyszła rozbudowa) rozszerzenia o dodatkowe porty. Zamawiający musi mieć możliwość rozszerzenia o dowolny moduł z poniższych opcji:
   a) co najmniej 2 porty Ethernet 10Gb i przyjmowania danych protokołami CIFS, NFS, BOOST, OST
   b) co najmniej 4 porty Ethernet 1Gb i przyjmowania danych protokołami CIFS, NFS, BOOST, OST

c) co najmniej2 porty FC 8Gb i przyjmowania danych protokołami VTL, BOOST, OST
d) co najmniej 4 porty 10GBase-T i przyjmowania danych protokołami CIFS,NFS, BOOST, OST

4. Urządzenie musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami czyli:
   - CIFS, NFS, OST, BOOST dla Ethernet
     oraz jednocześnie:
   - VTL, BOOST, OST dla FC (przyszła rozbduowa)
5. Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, BOOST, OST do pełnej pojemności urządzenia.
6. Oferowane urządzenie musi mieć możliwość (przyszła rozbudowa) emulacji następujących bibliotek taśmowych:
   a) StorageTek L180
   b) Adic Scalar i2000
   c) IBM 3500
7. Oferowane urządzenie musi mieć możliwość (przyszła rozbudowa) emulacji napędów taśmowych LTO1, LTO2, LTO3, LTO4
8. Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
9. Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości.
10. Proces de-duplikacji powinien odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
11. Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
12. Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, OST, BOOST) przechowywanych w obrębie całego urządzenia. Raz otrzymany i zapisany w urządzeniu fragment danych nie powinien nigdy więcej zostać zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.
13. Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy wirtualnymi bibliotekami. Blok danych otrzymany i zapisany w wirtualnej bibliotece A, nie powinien nigdy więcej zostać zapisany bez względu do jakiej wirtualnej biblioteki trafi.
14. Oferowane urządzenie musi wspierać z wykorzystaniem protokołu BOOST (OST - wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje backupowe
    a) EMC Avamar
    b) EMC NetWorker
    c) Symantec NetBackup
    d) Symantec Backup Exec
    e) Dell NetVault
    f) Dell vRanger
    g) HP Data Protector

h) VMware vSphere Data Protection Advanced
i) Veeam Backup and Replication

oraz aplikacje klasy Enterprise:

j) Oracle RMAN
k) Pivotal Greenplum
l) SAP
m) SAP HANA
n) IBM DB2
o) Microsoft SQL Server

15. Urządzenie musi zapewniać funkcjonalność pozwalającą na jednoczesny zapis minimum 60 strumieniami i jednocześnie w tym samym czasie odczyt danych minimum 15 strumieniami pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, OST, BOOST) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie. Wymienione wartości strumieni (60 dla zapisu i jednocześnie 15 strumieni dla odczytu) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. Wszystkie zapisywane strumienie muszą podlegać de-duplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.
16. Przestrzeń składowania zde-duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych.
17. Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.
18. Dostarczone urządzenie musi posiadać, co najmniej 17TB (podstawa liczenia 10) powierzchni netto (po odjęciu przestrzeni wykorzystywanej na zabezpieczenie RAID) przeznaczonej na przechowywanie unikalnych segmentów danych (backupów).
19. Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej).
20. Oferowane urządzenie musi umożliwiać replikację danych do drugiego urządzenia. Konfiguracja replikacji powinna być możliwa w trybie jeden do jednego i wiele do jednego. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Moduł replikacji nie musi być zawarty w ramach niniejszej oferty urządzenia, ma on być dostępny dla potrzeb przyszłej rozbudowy
21. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
22. W przypadku replikacji danych między dwoma urządzeniami muszą być możliwe do uzyskania jednocześnie następujące funkcjonalności:
    a) replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących
    b) replikacji podlegają tylko te fragmenty danych, które nie znajdują się w docelowym urządzeniu
    c) replikacja zarządzana tylko jest z poziomu aplikacji backupowej
    d) aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach
23. Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
24. Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6.
25. Każda grupa RAID 6 musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych.

26. Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność protokołami CIFS, NFS, co najmniej 3,5 TB/h (dane podawane przez producenta) oraz co najmniej 4,7 TB/h z wykorzystaniem de-duplikacji na źródle OST/BOOST (dane podawane przez producenta).
27. Oferowane urządzenie musi umożliwiać wykonywanie SnapShot'ów, czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania backupów / odtwarzania).
28. Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie.
29. Urządzenie musi pozwalać na podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia).
30. Dla każdej z logicznych części musi być możliwe zdefiniowanie blokady skasowania danych. Blokada skasowania danych musi uniemożliwiać usunięci pliku, modyfikację pliku w zadanym czasie. Brak możliwości zdjęcia blokady przed upływem ważności danych (compliance)
31. Urządzenie musi weryfikować dane po zapisie. Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie.
32. Urządzenie musi automatycznie (samoczynnie) wykonywać sprawdzanie spójności danych po zapisaniu danych da dysk oraz rozpoznawać i naprawiać błędy w locie. Każde zapisane na fizycznych dyskach dane muszą być odczytane i porównane z danymi otrzymanymi. Proces ten musi dziać się w locie – w trakcie zapisu danych przez urządzenie.
33. Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji)w procesie czyszczenia.
34. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracę procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu)
35. Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora)
36. Musi istnieć możliwość zdefiniowania czasu w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).
37. Musi być możliwość by usuwanie przeterminowanych danych (czyszczenie) odbywało się raz na tydzień minimalizując czas w którym backupy / odtworzenia narażone są na spowolnienie.
38. Urządzenie musi mieć możliwość zarządzania poprzez
    a) Interfejs graficzny dostępny z przeglądarki internetowej
    b) Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
39. Oprogramowanie do zarządzania musi rezydować oferowanym na urządzeniu de-duplikacyjnym.
40. Oferowany produkt musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych przed zapisaniem na dysk realizowany na poziomie urządzenia – długość klucza minimum 256-bit. Ewentualna licencja szyfrowania nie jest przedmiotem niniejszego zamówienia.
41. Urządzenie musi być rozwiązaniem kompletnym. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway z uwagi na brak miarodajnych danych dotyczących ich wydajności oraz dostępności. Zamawiający dopuszcza możliwość rozbudowy urządzenia przez dodanie modułów dyskowych

42. Dostarczone urządzenie musi stanowić całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt) i być serwisowane przez autoryzowany serwis producenta ze wsparciem na 3 lat w trybie 24/7/4

6.7.2. Serwery hiperkonwergentne – dla całości rozwiązania

Wykonawca ma obowiązek dostarczyć sprzęt nie gorszy niż wyspecyfikowany poniżej (w tabeli):

5 Node per DC: 2xE5-2650,384GB DDR4,15x1.2TB,1xSSD 120GB,1xSSD 1.6TB,2xSD 64GB; sumarycznie użytecznej przestrzeni dyskowej minimum 20TB		
Symbol	Opis	Ilość
	Architektura hiperkonwergentna	
HX-SP-240M4V1-FI	UCS SP HX240c Performance + Addnl 2xFI reqd	2
UCS-HX-FI48P	UCS SP Hyperflex System 6248 FI w/ 12p LIC	4
UCS-ACC-6248UP	UCS 6248UP Chassis Accessory Kit	4
N10-MGT012-HX	UCS Manager v2.2 for HyperFlex	4
UCS-FI-DL2	UCS 6248 Layer 2 Daughter Card	4
UCS-BLKE-6200	UCS 6200 Series Expansion Module Blank	4
UCS-FAN-6248UP	UCS 6248UP Fan Module	8
SFP-10G-SR	10GBASE-SR SFP Module	16
DS-SFP-FC8G-SW	8 Gbps Fibre Channel SW SFP+, LC	16
UCS-PSU-6248UP-AC	UCS 6248UP Power Supply/100-240VAC	8
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	8
HX-SP-240M4S-BV1	UCS SP HX240c Hyperflex System w/2xE52630v4,8x32Gmem	6
HX-CPU-E52650E	2.20 GHz E5-2650 v4/105W 12C/30MB Cache/DDR4 2400MHz	12
HX-MR-1X322RV-A	32GB DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4/1.2v	72
HX-HD12TB10K12G	1.2 TB 12G SAS 10K RPM SFF HDD	90
HX-SD120GBKS4-EB	120 GB 2.5 inch Enterprise Value 6G SATA SSD (boot)	6
UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 M4 and C240 M4 rack servers	6
HX-MLOM-CSC-02	Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+	6
UCSC-PSU2V2-1200W	1200W / 800W V2 AC Power Supply for 2U C-Series Servers	12
HX-SD-64G-S	64GB SD Card for UCS Servers	12
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	12
UCSC-PCI-1C-240M4	Right PCI Riser Bd (Riser 1) 2onbd SATA bootdrvs+ 2PCI slts	6
HX-SD16TB12S3-EP	1.6TB 2.5 inch Ent. Performance 6GSATA SSD(3X endurance)	6
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter	12
UCS-M4-V4-LBL	Cisco M4 - v4 CPU asset tab ID label (Auto-Expand)	6

N20-BBLKD	UCS 2.5 inch HDD blanking panel	48
HX240C-BZL-M4SX	HX240C M4 Security Bezel	6
UCSC-HS-C240M4	Heat sink for UCS C240 M4 rack servers	12
HX-SAS12GHBA	Cisco 12Gbps Modular (non-RAID) SAS HBA	6
HX-VSP-EPL-D	Factory Installed - VMware vSphere6 Ent Plus SW+Lic (2 CPU)	6
HX-VSP-EPL-DL	Factory Installed - VMware vSphere6 Enterprise Plus SW Dnld	6
HXDP-001-3YR=	Cisco HyperFlex HX Data Platform SW 3 year Subscription v1.8	6
HX-SP-240M4-V1	UCS SP HX240c Value + Addnl 2xFI reqd	4
HX-SP-240M4S-BV1	UCS SP HX240c Hyperflex System w/2xE52630v4,8x32Gmem	4
HX-CPU-E52650E	2.20 GHz E5-2650 v4/105W 12C/30MB Cache/DDR4 2400MHz	8
HX-MR-1X322RV-A	32GB DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4/1.2v	48
HX-HD12TB10K12G	1.2 TB 12G SAS 10K RPM SFF HDD	60
HX-SD120GBKS4-EB	120 GB 2.5 inch Enterprise Value 6G SATA SSD (boot)	4
UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 M4 and C240 M4 rack servers	4
HX-MLOM-CSC-02	Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+	4
UCSC-PSU2V2-1200W	1200W / 800W V2 AC Power Supply for 2U C-Series Servers	8
HX-SD-64G-S	64GB SD Card for UCS Servers	8
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	8
UCSC-PCI-1C-240M4	Right PCI Riser Bd (Riser 1) 2onbd SATA bootdrvs+ 2PCI slts	4
HX-SD16TB12S3-EP	1.6TB 2.5 inch Ent. Performance 6GSATA SSD(3X endurance)	4
SFP-H10GB-CU3M	10GBASE-CU SFP+ Cable 3 Meter	8
UCS-M4-V4-LBL	Cisco M4 - v4 CPU asset tab ID label (Auto-Expand)	4
N20-BBLKD	UCS 2.5 inch HDD blanking panel	32
HX240C-BZL-M4SX	HX240C M4 Security Bezel	4
UCSC-HS-C240M4	Heat sink for UCS C240 M4 rack servers	8
HX-SAS12GHBA	Cisco 12Gbps Modular (non-RAID) SAS HBA	4
HX-VSP-EPL-D	Factory Installed - VMware vSphere6 Ent Plus SW+Lic (2 CPU)	4
HX-VSP-EPL-DL	Factory Installed - VMware vSphere6 Enterprise Plus SW Dnld	4
HXDP-001-3YR=	Cisco HyperFlex HX Data Platform SW 3 year Subscription v1.8	4
SFP-H10GB-CU3M=	10GBASE-CU SFP+ Cable 3 Meter	8
	System do wirtualizacji	
VMW-VCS-STD-3S=	VMware vCenter 6 Server Standard, 3-yr Vmware SnS Reqd	2

VMW-VCS-STD-3YR	VMware vCenter 6 Server Standard SnS - 3 Year	2
UCS-VMW-TERMS	Acceptance of Terms, Standalone VMW License for UCS Servers	2

6.7.2.1. Wymagania minimalne dla architektury hiperkonwergentnej w przypadku zaproponowania rozwiązań równoważnych:

1. rozwiązanie klastruje się do minimum 8 węzłów pamięci masowej w pojedynczym klastrze
2. rozwiązanie oparte jest o węzły serwerowe x86 integrujące procesory, pamięć operacyjną i pamięć masową opartą o dyski HDD/SSD przy czym każdy z serwerów wyprowadza co najmniej dwa interfejsy 10 GigabitEthernet dla łączności w klastrze
3. węzły pamięci masowej umożliwiają wykorzystanie dysków SSD oraz HDD przy czym jest możliwa implementacja węzła wyposażonego jedynie w dyski SSD (tzw. All-Flash)
4. proponowane rozwiązanie zapewnia implementację wspólnego, rozproszonego zasobu pamięci masowej (datastore) w oparciu o cały klaster, dostępnego w taki sam sposób dla każdego węzła wchodzącego w skład klastra
5. rozwiązanie zapewnia prezentację wspólnego zasobu pamięci masowej (datastore) również dla serwerów nie wyposażonych w dyski SSD/HDD (bezdyskowych) dołączonych do klastra
6. rozwiązanie zapewnia replikację każdego segmentu danych na przynajmniej trzech różnych węzłach
7. rozwiązanie jest skalowalne (scale-out) czyli rozbudowa jest zapewniona poprzez bezprzerwowe dołożenie kolejnego węzła do klastra
8. rozwiązanie jest oparte na serwerach maksymalnie dwuprocesorowych, tak aby w wyniku awarii jednego z węzłów klastra, spadek wydajności całości był jak najmniejszy;
9. rozwiązania zapewnia pełną ciągłość i funkcjonalność działania w wypadku awarii lub całkowitej niedostępności pojedynczego węzła
10. rozwiązanie zapewnia pełną ciągłość i funkcjonalność działania w wypadku jednoczesnej awarii pojedynczych dysków w dwóch węzłach
11. rozwiązanie posiada możliwość kontrolowanego wyłączania pojedynczego węzła z klastra poprzez przełączanie go w tryb utrzymaniowy (maintenance)
12. rozwiązanie integruje się z infrastrukturą wirtualizacyjną pracującą pod kontrolą VMware vSphere; odpowiednie licencje VMware vSphere Enterprise Plus na ilość procesorów, obejmującą wszystkie serwery klastra, muszą być zapewnione w oferowanym rozwiązaniu
13. rozwiązanie posiada możliwość administracji z poziomu vCenter Web Client; odpowiednie licencje vCenter muszą być zapewnione w oferowanym rozwiązaniu
14. rozwiązanie posiada możliwość weryfikacji i diagnozowania działania poprzez dedykowany interfejs linii komend (CLI)
15. rozwiązanie posiada dostępne publicznie potwierdzenie kompatybilności z mechanizmami replikacji i archiwizacji opartymi o rozwiązania Veeam
16. rozwiązanie zapewnia zwiększenie wydajności operacji wejścia/wyjścia za pomocą architektury Cache implementowanej w oparciu o pamieć SSD;

17. rozwiązanie zapewnia deduplikację i kompresję maszyn wirtualnych, implementowaną zarówno dla dysków Flash jak i dysków magnetycznych HDD; odpowiednie komponenty sprzętowe bądź licencyjne muszą być zapewnione w oferowanym rozwiązaniu;
18. rozwiązanie posiada funkcjonalność zoptymalizowanego klonowania maszyn wirtualnych przy czym jest możliwe wygenerowanie co najmniej 200 klonów maszyny w ramach jednoczesnej operacji; klonowanie jest możliwe dla maszyn posiadających kopie migawkowe (snapshot)
19. architektura rozwiązania umożliwia maszynom wirtualnym korzystanie również z innych, znajdujacych się poza klasterem zasobów pamięci masowej udostępnianych poprzez protokoły FC, iSCSCI, NFS
20. wszystkie licencje dla architektury fizycznej klastra zapewnione są dla jej maksymalnej pojemności i rozmiaru klastra
21. wszystkie licencje dla architektury fizycznej klastra zapewnione są tak aby obejmować całkowitą funkcjonalność rozwiązania
22. Rozwiązanie musi być identyczne dla dwóch ośrodków przetwarzania danych
23. Serwery w jednym klastrze muszą zapewniać łącznie:
    a) Minimum 96 rdzeni CPU
    b) Minimum 1.5 TB RAM użytecznej pamięci
    c) Minimum 20 TB użytecznej przestrzeni dyskowej z możliwością rozszerzenia to 30 TB

Przy czym, powyższe parametry muszą być spełnione przy całkowitej awarii jednego z serwerów w klastrze.

6.7.2.2. Wymagania minimalne dla systemu wirtualizacji w przypadku zaproponowania rozwiązań równoważnych:

1. licencje na wirtualizator muszą obejmować ilość procesorów, obejmującą wszystkie serwery klastra.

Konsolidacja

2. Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego.
3. Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
4. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest możliwość przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 4TB pamięci operacyjnej.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych.
7. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
8. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
9. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, SLES 11, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris wersja 10 dla platformy x86,

NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04, SCO OpenServer, SCO Unixware, Mac OS X.

10. Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7 a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej.
11. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta i za pomocą przeglądarek, minimum IE i Firefox.
12. Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
13. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
14. Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej na serwerze Syslog. Serwer Syslog w dowolnej implementacji musi stanowić integralną część rozwiązania.
15. Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
16. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
17. Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
18. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
19. Kopie zapasowe muszą być składowane z wykorzystaniem technik deduplikacji danych.
20. Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.
21. Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii.
22. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
23. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
24. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
25. Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
26. Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 62TB.

27. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
28. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
29. Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
30. Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
31. Rozwiązanie musi gwarantować współczynnik RPO na poziomie minimum 5 minut
32. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum.
33. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
34. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
35. System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE.
36. Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją.
37. Konsola zarządzania platformą wirtualizacji musi umożliwiać centralną konfigurację przełącznika rozproszonego a mechanizmy wewnętrzne muszą zapewniać propagację tej konfiguracji do wszystkich serwerów fizycznych tworzących wzajemnie ten przełącznik.
38. Platforma wirtualizacji powinna w ramach przełącznika sieciowego musi zapewniać możliwość integracji z produktami (przełącznikami wirtualnymi) firm trzecich, tak aby umożliwić granularną delegację zadań w zakresie zarządzania konfiguracją sieci do zespołów sieciowych.
39. Przełącznik rozproszony musi współpracować z protokołem NetFlow.
40. Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port.
41. Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej.
42. System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.

Wysoka dostępność

43. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami virtualnych przełączników

sieciowych, pomiędzy Centrami Przetwarzania Danych oraz pomiędzy Centralnymi Konsolami Zarządzającymi platformami wirtualnymi.

44. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.
45. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
46. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
47. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji.
48. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
49. Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.
50. Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.
51. System musi umożliwiać kontrolę dostępu sieciowego do obszarów wrażliwych wirtualnego centrum danych takiego jak DMZ lub serwery z danymi wrażliwymi podlegające zgodności z przepisami PCI lub SOX w obszarze środowiska wirtualnego.

Równoważenie obciążenia i przestoje serwisowe

52. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi, wolumenami dyskowymi, klastrami, centrami przetwarzania danych bez przerywania pracy usług.
53. Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
54. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych.
55. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.
56. System musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką.
57. System musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone.

6.8. Pamięć RAM – 6 szt.

Zamawiający posiada w swoim środowisku urządzenie UCSC-C220-M3L o numerze seryjnym FCH 1909V03C, w którym zainstalowane są pamięci 8GB (DDR3-1600MHz RDimmIPC3-12800/2R/x4/1.35V (Product ID: UCS-MR-1X082RY-A). Zamawiający wymaga dostarczenia dodatkowo sześciu kości pamięci każda po 8 GB. Ze względu na wymagania serwisowe producenta urządzenia Cisco UCS wymagane jest dostarczenie oryginalnych kości pamięci tego producenta.

6.9. Wkładki SFP – w sumie 12 szt.

Zamawiający wymaga dostarczenia 4 szt. wkładek SFP-10G-ER-S (10GBASE-ER SFP Module, Enterprise-Class) oraz 8 szt. wkładek GLC-TE (1000BASE-T SFP transceiver module for Category 5 copper wire). Ze względu na wymagania serwisowe producenta urządzenia Cisco Nexus 7706 wymagane jest dostarczenie oryginalnych wkładek tego producenta.

6.10. Urządzenia nowej generacji pełniące funkcję ściany ogniowej oraz wykrywania i zapobiegania włamaniom– 2 szt.

Wykonawca ma obowiązek dostarczyć sprzęt nie gorszy niż wyspecyfikowany poniżej (w tabeli):

Symbol	Opis	Ilość
FPR4110-BUN	Cisco Firepower 4110 Master Bundle	1
FPR4110-NGIPS-K9	Cisco Firepower 4110 NGIPS Appliance, 1U, 2 x NetMod Bays	1
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	2
SF-FXOS4K-2.0-K9	Firepower Extensible Operating System (FXOS) for FPR4K	1
SF-FPR-TD6.1-K9	Cisco Firepower Threat Defense software v6.1	1
SFP-10G-SR	10GBASE-SR SFP Module	6
FPR4K-SSD200	Firepower 4000 Series SSD for FPR-4110/4120	1
FPR4K-SSD-BBLKD	Firepower 4000 Series SSD Slot Carrier	1
FPR4K-ACC-KIT	FPR4K Hardware Accessory Kit (Rack Mounts, Cables)	1
FPR4K-FAN	Firepower 4000 Series Fan	6
FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	1
FPR4K-RACK-MNT	Firepower 4000 Series Rack Mount Kit	1
FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	1
FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	1
FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	1
L-FPR4110T-T=	Cisco FPR4110 Threat Defense Threat Protection License	1
L-FPR4110T-T-3Y	Cisco FPR4110 Threat Defense Threat Protection 3Y Subs	1

Wymagania minimalne w przypadku zaproponowania rozwiązania równoważnego:

Architektura urządzenia, obudowa, interfejsy

1. Urządzenie powinno być dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia
2. Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall)
3. Urządzenie powinno być wyposażone w co najmniej 8 portów 10 Gigabit Ethernet SFP+ oraz dwa sloty na moduły rozszerzeń umożliwiające dalszą rozbudowę o porty 10 Gigabit Ethernet SFP+ (co najmniej 8) oraz 40Gigabit Ethernet QSFP+ (co najmniej 4 porty), i być dostarczone z co najmniej 6 wkładkami SFP typu 10GBASE-SR
4. Urządzenie musi obsługiwać interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1.000 sieci VLAN
5. Urządzenie powinno być wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band
6. Urządzenie powinno być wyposażone w port USB 2.0
7. Urządzenie musi być dostarczone z co najmniej 2 zasilaczami dla zasilania w sposób redundantny prądem przemiennym 230V
8. Urządzenie musi mieć możliwość montażu w szafie rack 19" (wymagane jest dołączenie ew. niezbędnych elementów montażowych)
9. Wysokość urządzenia max 1RU

Parametry wydajnościowe

10. Wymagana przepustowość teoretyczna urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 12Gb/s, a dla modułów AVC oraz systemu IPS na poziomie 10Gb/s
11. Wymagana wydajność dla ruchu rzeczywistego http dla modułów AVC lub IPS na poziomie 4Gb/s
12. Wymagana maksymalna liczba sesji (z kontrolą aplikacji) na poziomie 4.500.000 z możliwością zestawiania co najmniej 60.000 nowych połączeń na sekundę

Funkcjonalność urządzenia

13. Urządzenie nie powinno posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
14. Urządzenie powinno mieć możliwość uruchomienia w trybie firewall'a L3, jak i w trybie transparentym
15. Urządzenie powinno obsługiwać routing statyczny i dynamiczny (RIP, OSPF, BGP)
16. Urządzenie powinno posiadać możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory
17. Urządzenie powinno obsługiwać funkcjonalność Network Address Translation (NAT oraz PAT)
18. Urządzenie powinno zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standy
19. Urządzenie powinno zapewniać funkcjonalność tzw. Firewall'a Next-Generation w zakresie:

a. systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control)
b. systemu IPS (z wymaganą licencją i/lub subskrypcją)
c. systemu ochrony przed malware (dopuszcza się możliwość włączenia funkcjonalności poprzez dostawę odpowiedniej licencji, jednak nie jest ona wymagana w tym postępowaniu – dostarczany system musi zapewniać jedynie możliwość włączenia takiej funkcji)
d. systemu filtracji ruchu w oparciu o URL (dopuszcza się możliwość włączenia funkcjonalności poprzez dostawę odpowiedniej licencji, jednak nie jest ona wymagana w tym postępowaniu – dostarczany system musi zapewniać jedynie możliwość włączenia takiej funkcji)

20. System powinien posiadać możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a. Wiedza o użytkownikach – uwierzytelnienie
    b. Wiedza o urządzeniach – pasywne skanowanie ruchu
    c. Wiedza o urządzeniach mobilnych
    d. Wiedza o aplikacjach wykorzystywanych po stronie klienta
    e. Wiedza o podatnościach
    f. Wiedza o bieżących zagrożeniach
    g. Baza danych URL
21. System powinien posiadać otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM
22. System powinien mieć możliwość wykrywania aplikacji AVC zapewniający:
    a. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji
    b. możliwość tworzenia profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług
    c. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
    d. współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach
23. System musi być wyposażony w IPS zapewniający:
    a. możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system)
    b. możliwość pracy w trybie pasywnym (IDS)
    c. możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
        i. złośliwe oprogramowanie
        ii. skanowanie sieci
        iii. ataki na usługę VoIP
        iv. próby przepełnienia bufora
        v. ataki na aplikacje P2P
        vi. zagrożenia dnia zerowego, itp.
    d. możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna)
    e. wiele sposobów wykrywania zagrożeń w tym:

i. sygnatury ataków opartych na exploitach
ii. reguły oparte na zagrożeniach
iii. mechanizm wykrywania anomalii w protokołach
iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego

f. możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
g. mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives)
h. możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń
i. wiele możliwości reakcji na zdarzenia w tym takie, jak:
    i. tylko monitorowanie
    ii. blokowanie ruchu zawierającego zagrożenia
    iii. zastąpienie zawartości pakietów
    iv. zapisywanie pakietów
j. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6
k. możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
    i. systemach operacyjnych
    ii. serwisach
    iii. otwartych portach, aplikacjach
    iv. zagrożeniach
l. możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych
m. możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.
n. możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
o. możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego
p. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
q. możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie
r. obsługę reguł Snort
s. możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS
t. mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise)
u. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa

24. System filtracji URL zapewniający (dopuszcza się możliwość włączenia funkcjonalności poprzez dostawę odpowiedniej licencji, jednak nie jest ona wymagana w tym postępowaniu – dostarczany system musi zapewniać jedynie możliwość włączenia takiej funkcji):
    a. kategoryzację stron – w co najmniej 70 kategoriach
    b. bazę URL o wielkości nie mniejszej niż 250 mln URL
25. Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:
    a. pliki systemowe
    b. pliki graficzne
    c. pliki PDF
    d. pliki wykonywalne
    e. pliki multimedialne
    f. pliki pakietu Office
    g. pliki skompresowane
26. Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download
27. Urządzenie musi mieć wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez (dopuszcza się możliwość włączenia funkcjonalności poprzez dostawę odpowiedniej licencji, jednak nie jest ona wymagana w tym postępowaniu – dostarczany system musi zapewniać jedynie możliwość włączenia takiej funkcji)
    a. sprawdzenie reputacji plików w systemie globalnym
    b. sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze)
    c. statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu
28. Urządzenie musi zapewniać możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach
    a. pliki wolne od złośliwego kodu
    b. pliki zawierające złośliwy kod
    c. pliki podejrzane
    d. pliki o własnej, zdefiniowanej przez użytkownika kategorii
29. Urządzenie musi posiadać podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna)
30. Urządzenie ma mieć możliwość rozbudowy podsystemu antimalware o agenta instalowanego na stacjach roboczych i serwerach. Konsola zarządzająca posiadająca możliwość wyświetlenia szczegółowej trajektorii transferu danego pliku po monitorowanej sieci oraz korelacji zdarzeń przychodzących z rozwiązania antymalware rezydującego na serwerach i stacjach roboczych
31. Urządzenie ma mieć możliwość zarządzania poprzez system opisany w p-cie 6.4
32. Urządzenie musi zostać objęte 3-letnim serwisem świadczonym bezpośrednio przez producenta lub autoryzowanego partnera serwisowego producenta w reżimie 24x7x4 uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia. Dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez okres 3 lat

33. Wraz z urządzeniem musi być dostarczona licencja na okres 3 lat na funkcjonalność IPS opisaną w pkt. 23

7. Monitor min. 55'' – 1 szt.

1. Rodzaj ekranu – LED
2. Ekran – min. 55 cali/139 cm
3. Rozdzielczość – min. 3840 x 2160
4. Częstotliwość odświeżania – min. 600Hz
5. Kontrast dynamiczny – min. 1 000 000 : 1
6. Jasność ekranu – min. 280 cd/m2
7. Interfejsy wejścia/wyjścia:
   a) złącze HDMI – min. 3 szt.
   b) złącze USB – min. 2 szt.
   c) złącze Ethernet (LAN) – min. 1 szt.
   d) komunikacja dodatkowa: Bluetooth, czytnik kart pamięci SD, SDHC, SDXC, cyfrowe wyjście optyczne, złącze CI, złącze EURO, wejście komponentowe
8. Waga z podstawą – maksymalnie 14,2 kg
9. Waga bez podstawy – maksymalnie 13,9 kg
10. Wymiary z podstawą (szer. x wys.x gł.) - 123,7 x 76,8 x 22,9 cm
11. Wymiary bez podstawy (szer. x wys.x gł.) - 123,7 x 72,6 x 6,8 cm
12. Możliwość montażu na ścianie - VESA 600x300 mm
13. Efektywność energetyczna :
    a) zasilanie - 220 - 240 V 50/60 Hz
    b) klasa energetyczna – A
    c) pobór mocy (tryb włączenia) - 110 W
    d) pobór mocy (tryb czuwania) - 0,50 W
    e) pobór mocy (max) - 180 W
14. Wyposażenie i akcesoria:
    a) pilot + baterie
    b) podstawa
    c) adapter AV
    d) adapter EURO
    e) adapter komponent
    f) instrukcja obsługi w języku polskim
    g) karta gwarancyjna
15. Znak zgodności – CE
16. Wraz z monitorem należy dostarczyć bezprzewodowy zestaw klawiatura/mysz.
17. Wraz z monitorem należy dostarczyć urządzenie/moduł z systemem umożliwiającym cykliczne wyświetlanie danych z systemów zarządzania oraz z możliwością uruchomienia zdalnego pulpitu urządzeń będących w infrastrukturze Zamawiającego na potrzeby zarządzania.

8. Konsola administracyjna – 2 szt. na potrzeby testów penetracyjnych wraz ze stacjami dokującymi

Nazwa	Wymagane parametry techniczne
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych,

	dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Przekątna Ekrenu	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości: 15.6" UHD (3840x2160) IGZO3, jasność min. 360nits, kontrast 1000:1, maksymalny rozmiar pixel'a matrycy 0,10 mm, (100% Adobe color gamut)
Procesor	Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 8770 punktów Passmark CPU Mark.Wynik dostępny na stronie : http://www.passmark.com/products/pt.htm
Płyta główna	Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora. Zaprojektowana na zlecenie producenta i oznaczona trwale na etapie produkcji nazwą lub logiem producenta oferowanego komputera.
Pamięć RAM	16GB (1x16GB) DDR4 SDRAM 2133MHz możliwość rozbudowy do min 32GB,
Pamięć masowa	min. 1TB SATA oraz 128GB SSD M.2 Kontroler pamięci masowej musi umożliwiać skonfigurowania RAID
Karta graficzna	Układ graficzny z własną niewspółdzieloną pamięcią 2GB DDR5, Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 1945 punktów w G3D Rating, wynik dostępny na stronie : http://www.videocardbenchmark.net/gpu_list.php
Klawiatura	Klawiatura wyspowa z powłoka antybakteryjna, min. 80 klawiszy, z wbudowanym w klawiaturze podświetleniem z możliwością manualnej regulacji zarówno w BIOS, jak i z pod systemu operacyjnego, (układ US -QWERTY),
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowany min. 1 głośnik Kamera internetowa z mikrofonem, o rozdzielczości min. 1280x720 pixels trwale zainstalowana w obudowie matrycy.
Bateria i zasilanie	Min. 3-cell [min. 56Whr]. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy min. 130W.
Waga	Waga max 1,9kg z baterią
Obudowa	Szkielet obudowy wykonany z wzmocnionego włókna węglowego, zawiasy notebooka wykonane ze wzmacnianego metalu, dookoła matrycy gumowe uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią.
Wirtualizacja	Sprzętowe wsparcie technologi wirtualizacji procesorow, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i myszy lub urządzenia wskazującego zintegrowanego (wmontowanego na

	stałe) w oferowanym urządzeniu Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: ▪ wersji BIOS, ▪ nr seryjnym komputera, ▪ numerze wpisanym i nadanym przez administratora (o ile został wpisany, jeśli brak – wymaga się wolnego pola), ▪ dacie produkcji komputera, ▪ dacie wysyłki komputera z fabryki, ▪ całkowitej wielkości zainstalowanej pamięci RAM, ▪ prędkości zainstalowanej pamięci RAM, ▪ technologii wykonania pamięci RAM, ▪ sposobu obsadzenia slotów DIMM, ▪ typie zainstalowanego procesora, ▪ liczbie rdzeni procesora, ▪ minimalnej prędkości zegara procesora, ▪ maksymalnej prędkości zegara procesora, ▪ wielkości pamięci podręcznej procesora L2 cache, ▪ wielkości pamięci podręcznej procesora L3 cache, ▪ czy jest aktywna w zainstalowanym procesorze technologia wielowątkowości, ▪ technologii 64-bit procesora, ▪ zainstalowanych i podpiętych HDD, ▪ kontrolerze video [dotyczy tylko zintegrowanej karty], ▪ wersji BIOS kontrolera video, ▪ pamięci kontrolera video przydzielonej na poziomie BIOS'u, ▪ typie zainstalowanego w komputerze panelu LCD (wielkość matrycy w calach), ▪ natywnej rozdzielczości zainstalowanego w komputerze panelu LCD, ▪ kontrolerze audio, ▪ zainstalowanej karcie Wifi (jeśli brak w wymaganiach specyfikacji dopuszcza się puste pole), ▪ zainstalowanym Bluetooth (jeśli brak w wymaganiach specyfikacji dopuszcza się puste pole), ▪ zainstalowanym modemie dla internetu bezprzewodowego (jeśli brak w wymaganiach specyfikacji dopuszcza się puste pole), Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi.

	Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Dopuszcza się, aby po wprowadzeniu hasła systemowego była możliwość jedynie zmiany hasła systemowego i hasła dla dysku twardego (o ile zostało zdefiniowane przez administratora). Możliwość włączenia/wyłączenia technologii raportowania i zgłaszania błędu zainstalowanego dysku twardego podczas uruchamiania systemu, technologia ta jest analizą samokontrolną. Możliwość włączenia/wyłączenia zintegrowanego kontrolera USB, Możliwość włączenia/wyłączenia portu Typ-C, (funkcja zaimplementowana w BIOS na stałe, aktywna przy zainstalowanym złączu), Możliwość włączenia/wyłączenia dosilenia portu USB, Możliwość włączenia/wyłączenia zintegrowanego kontrolera audio, Możliwość włączenia/wyłączenia podświetlenia wbudowanego w klawiaturę [funkcja zaimplementowana na stałe w BIOS, ale aktywna przy zainstalowanej klawiaturze z wbudowanym podświetleniem], Możliwość włączenia/wyłączenia urządzeń : - czujnika upadku HDD, - kamery [funkcja zaimplementowana na stałe w BIOS ale aktywna przy zainstalowanej kamerze], - mikrofonu, - głośnika, - czytnika multimedialnych kart, Możliwość ustawienia czytnika kart multimedialnych w opcji tylko odczyt, Możliwość włączenia/wyłączenia szybkiego ładownia baterii, Możliwość włączenia/wyłączenia funkcjonalności Wake On LAN/WLAN – zdalne uruchomienie komputera za pośrednictwem sieci LAN i WLAN – min. trzy opcje do wyboru: tylko LAN, tylko WLAN, LAN oraz WLAN, Możliwość włączenia/wyłączenia hasła dla dysku twardego, Możliwość ustawienia jasności matrycy podczas pracy, oddzielnie dla baterii i dla zasilacza, Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia Virtual Machine Monitor (VMM) [funkcja zaimplementowana na stałe w BIOS, ale aktywna przy procesorze w pełni wspierającym VMM], Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia funkcji VT dla Direct I/O [funkcja zaimplementowana na stałe w BIOS, ale aktywna przy procesorze w pełni wspierającym funkcję VT dla

	Direct I/O], Możliwość ręcznego zdefiniowania zapotrzebowania na ilość rdzeni procesora dla aplikacji, a w szczególności dla starszych, mających problemy z nowymi procesorami, wymagane min. dwa tryby : - aktywny jeden rdzeń, - aktywne dwa rdzenie, - aktywne trzy rdzenie, Możliwość ręcznego włączenia/wyłączenia funkcji, która pozwalająca na dynamiczną zmianę wartości mnożnika i napięcia [funkcja związana z architekturą procesora, nie dopuszcza się overclokingu, zaimplementowana na stałe w BIOS, ale aktywna przy procesorze w pełni wspierającym], Możliwość ręcznego włączenia/wyłączenia funkcji uśpienia procesora dla systemu operacyjnego w trybie bezczynności w celu zwiększenia oszczędności energii [funkcja zaimplementowana na stałe w BIOS, ale aktywna przy procesorze w pełni wspierającym], Możliwość ręcznego włączenia/wyłączenia funkcji procesora, która automatycznie zwiększa taktowanie procesora, gdy komputerowi potrzebna jest wyższa prędkość obliczeniowa [funkcja zaimplementowana na stałe w BIOS, ale aktywna przy procesorze w pełni wspierającym], Możliwość ręcznego włączenia/wyłączenia funkcji procesora, która automatycznie zwiększa wydajność obliczeń prowadzonych równolegle [funkcja zaimplementowana na stałe w BIOS, ale aktywna przy procesorze w pełni wspierającym], Możliwość przypisania w BIOS numeru nadawanego przez Administratora/Użytkownika oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. - Możliwość włączenia/wyłączenia układu TPM. - Możliwość ustawienia trybu Fastboot w opcji : minimalnej – następuje skrócony czas rozruchu komputera z pominięciem pełnej weryfikacji inicjalizacji konfiguracji sprzętowej gruntownej - podczas rozruchu komputera następuje pełna weryfikacja i inicjalizacja konfiguracji sprzętowej, Funkcja zbierania i zapisywania logów, Możliwość przeglądania i kasowania zdarzeń przebiegu procedury POST. Funkcja ta obejmuje datę i godzinę zdarzeń, Możliwość włączenia/wyłączenia zabezpieczenie wykrywające uszkodzenie zasilacza lub wykrycie podłączenia zasilacza o niewłaściwym min. napięciu, Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość zdefiniowania automatycznego uruchamiania komputera w min. dwóch trybach : codziennie lub w wybrane dni tygodnia, Możliwość włączenia/wyłączenia wzbudzania komputera za

	pośrednictwem portów USB, Możliwość włączenia/wyłączenia funkcji umożliwiającej dokonywanie downgrade BIOS, Możliwość włączenia/wyłączenia funkcji tworzenia recovery BIOS na dysku twardym, Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia min. : - uruchamianie z system zainstalowanego na HDD, - uruchamianie systemy z urządzeń zewnętrznych typu HDD-USB, USB Pendrive, CDRW-USB, - uruchamianie systemu z karty SD (funkcja aktywna automatycznie po zainstalowaniu karty SD w czytniku), - uruchomienie graficznego systemu diagnostycznego, - wejścia do BIOS, - upgrade BIOS bez konieczności uruchamiania systemu operacyjnego, - zmiany sposobu boot'owania z Legacy na UEFI lub z UEFI na Legacy bez konieczności wchodzenia do BIOS.
Certyfikaty	Certyfikat ISO9001:2008 dla producenta sprzętu (należy załączyć do oferty) Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty) Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki Potwierdzenie kompatybilności komputera na stronie Windows Logo'd Products List na daną platformę systemową (wydruk ze strony) EnergyStar 6.1 – załączyć do oferty certyfikat lub oświadczenie wykonawcy opatrzone numerem postępowania i poparte oświadczeniem producenta.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 18dB (załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta)
Diagnostyka	Wbudowany system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony min. o funkcjonalność : - wykaz wszystkich zainstalowanych komponentów z numerami seryjnym dla : - płyty głównej, - pamięci - HDD - kamery

	- modemu 3G/LTE - dokładnych informacji o zainstalowanej baterii, a w szczególności : - ilości wykonanych cykli ładowania baterii - temperaturze baterii - podanej w % wartości żywotności baterii - Test podzespołów : - test podpiętych kabli, - test magistrali PCIe - test matrycy LCD, - test głośnika - test dysku twardego - test partycji rozruchowej systemu OS - test portów USB - test kamery - test karty graficznej - test baterii - test zasilacza - test wentylatora procesora - test procesora - test pamięci Wbudowany wizualny system diagnostyczny oparty na sygnalizacji za pomocą diod sygnalizujących pracę HDD, zailania, WiFi umożliwiający wykrycie bez konieczności uruchamiania systemu operacyjnego min.: - awarii procesora, - błędu pamięci, - problemu z inicjalizacją systemu OS z HDD, - awarii karty graficznej, - awarii portów USB, - braku pamięci, - problemu z panelem LCD - problemu z zainicjowaniem/obsługą pamięci
Zarządzanie	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: • monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; • zdalną konfigurację ustawień BIOS, • zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; • zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie;

	• zapis i przechowywanie dodatkowych informacji dot. np. o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji z wbudowanej pamięci nieulotnej; • technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (http://www.dmtf.org/standards/wsman) oraz DASH 1.0.0 (http://www.dmtf.org/standards/mgmt/dash/) • nawiazywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS; • wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika systemu sprzętowego zarządzania zdalnego; • sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji; • ww. wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym - powinna pozwalać na konfigurację parametrów funkcji zarządzania (m.in. parametrów kont uprawnionych do zarządzania sprzętowego) każdym z następujących mechanizmów: - lokalnie (na komputerze zarządzanym), bez udziału systemu operacyjnego - tj. manualnie z poziomu modułu BIOS, - lokalnie (na komputerze zarządzanym), bez udziału systemu operacyjnego - tj. z poziomu modułu BIOS przy użyciu pliku parametrów konfiguracji na nośniku USB. Należy dostarczyć odpowiednie narzędzie/oprogramowanie do tworzenia pliku parametrów konfiguracji na nośnik USB, - zdalnie poprzez sieć LAN z wykorzystaniem szyfrowanego połączenia – za pomocą narzędzia/oprogramowania konfigurującego. Szyfracja połączenia LAN powinna pozwalać na wykorzystanie zarówno definiowanego przez użytkownika klucza symetrycznego PSK lub wbudowanych w technologię certyfikatów cyfrowych /kluczy asymetrycznych, Należy dostarczyć odpowiednie narzędzie do definiowania pliku parametrów konfiguracji oraz narzędzie/oprogramowanie konfigurujące, - lokalnie (na komputerze zarządzanym) z poziomu systemu operacyjnego przy użyciu odpowiedniego narzędzia. Należy dostarczyć odpowiednie narzędzie do definiowania pliku parametrów konfiguracji oraz narzędzie/oprogramowanie konfigurujące.

	Sprzętowe wsparcie technologii weryfikacji poprawności podpisu cyfrowego wykonywanego kodu oprogramowania, oraz sprzętowa izolacja segmentów pamięci dla kodu wykonywanego w trybie zaufanym wbudowane w procesor, kontroler pamięci, chipset I/O. Wbudowana w płytę główna technologia zabezpieczająca pozwalająca na sprzętową, trwałą blokadę możliwości uruchomienia komputera – po jego zablokowaniu zdalnie poprzez sieć Internet lub lokalnie w po definiowalnym przez użytkownika czasie. Technologia ta powinna zapewniać możliwość odblokowania komputera przez legalnego użytkownika po poprawnej autoryzacji predefiniowanym kodem numerycznym lub hasłem.kodem jednorazowego użytku. Wbudowany w płyte główną dodatkowy mikroprocesor, niezależny od głownego procesora laptopa, pozwalający na generowanie hasła jednorazowego użytku (OTP –One Time Password) n.p. z wykorzystaniem OATH.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Czujnik spadania zintegrowany z płytą główną działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy. Złącze typu Kensington Lock.
System operacyjny	Zainstalowany system operacyjny Windows 10 Professional lub + nośnik, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. Oferowany dostarczony system jak i również przy reinstalacji nie może wymagać aktywacji klucza licencyjnego za pośrednictwem telefonu i Internetu).
Dodatkowe oprogramowanie dodatkowe	Zainstalowane oprogramowanie z bezterminową licencją do wykonywania aktualizacji systemu i jego zasobów umożliwiające : - określenie preferencji aktualizacji, - ustawienie priorytetu aktualizacji, - użycia opcji planowania aktualizacji bieżących wersji sterowników, Dołączone do oferowanego komputera oprogramowanie

	producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: a. o poprawkach i usprawnieniach dotyczących aktualizacji, b. dacie wydania ostatniej aktualizacji, c. priorytecie aktualizacji, d. zgodność z systemami operacyjnymi, e. jakiego komponentu sprzętu dotyczy aktualizacja, f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne, - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga, - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr), - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania), - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml, - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. Oprogramowanie producenta komputera z licencją bezterminową dedykowane dla zarządzania baterią, dostępne z poziomu system operacyjnego dla użytkownika oraz dla administratora z poziomu zdalengo zarządzania bez potrzeby konfigurowania ustawień w BIOS. Oprogramowanie musi umożliwiać co najmniej odczytanie Informacji o :

	- Żywotności baterii , - % (procentowym) statusie naładowania baterii, - Ustawionej opcji zarządzania baterią w BIOS'ie, - Numerze seryjnym baterii, Musi umożliwiać ustawienie zaawansowanego planu ładowania baterii w zakresie: - poszczególny dzień tygodnia (określenie do godziny i minuty czasu ładowania), - zdefiniowanie harmonogramu tylko dla jednego dnia i powielenia go dla pozostałych, - możliwość ustawienia zakresu czasowego pracy tylko na samej baterii nawet kiedy jest podpięte zasilanie, - możliwość ustawienia zakresu czasowego pracy tylko na zasilaniu sieciowym mimo naładowania baterii w 100%, bez włączania ładowania i doładowywania, - możliwość ustawienia zakresu czasowego pracy tylko na zasilaniu sieciowym wraz z jednoczesnym ładowaniem baterii, Musi posiadać Możliwość ustawienia automatycznego przywrócenia zasilania sieciowego w przypadku osiągnięcia krytycznej % wydajności baterii określonej przez administratora bądź użytkowanika, Zarządzanie termiczne odpowiedzialne za wydajność procesora, głośność pracy wentylatora oraz kontrolowanie za pomocą czujnika termicznego wewnętrznej temperatury, możliwość ustawienia opcji w minimum czterech wariantach (np. zrównoważony, chłodzenie, cichy bądź wydajny) zdefiniowanych przez oprogramowanie, Zainstalowane oprogramowanie z bezterminową licencją tworzenia kopii zapasowych i przywracania danych, umożliwiające : - tworzenie OS media - tworzenie kopii zapasowych na wskazanych prze użytkownika lokalizacjach [min. lokalnie, sieć, chmura].
Porty i złącza	Wbudowane porty i złącza : - 1x HDMI 1.4 - 2x USB 3.0 - czytnik kart multimedialny wspierający karty SD 4.0 - współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo - touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów - Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN z Bluetooth 4.1LE obsługująca łącznie standardy IEEE 802.11 AC
Dodatkowe akcesoria	- stacja dokująca, - mysz i klawiatura bezprzewodowa - plecak

9. **Świadczenie Usługi Serwisu i Gwarancji - Minimalne Wymagania Dla Urządzeń**
   1) O ile wymagania szczegółowe nie specyfikują inaczej, na dostarczane Urządzenia musi być udzielona min. 36 miesięczna gwarancja. Zamawiający wymaga, aby usługa gwarancyjna na Urządzenia była, przez cały okres jej trwania, świadczona na podstawie wykupionego wsparcia producenta Urządzeń, to jest by zapewniona była naprawa lub wymiana Urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta
   2) Zamawiający wymaga, aby Wykonawca posiadał status partnera producenta dostarczanych Urządzeń i był jego autoryzowanym dostawcą (z pominięciem urządzeń opisanych w punkcie 7 i 8).
   3) Wszystkie dostarczone i zastosowane przez wykonawcę Urządzenia będą fabrycznie nowe (nie będą używane) i będą pochodziły z bieżącej produkcji, tzn. nie będą starsze niż 6 miesięcy. Wykonawca na etapie realizacji umowy zobowiązuje się dostarczyć Zamawiającemu oświadczenie producenta(ów) potwierdzające datę produkcji urządzeń.
   4) Wszystkie wkładki i moduły dostarczone wraz z urządzeniami, będą pochodziły od jednego producenta. Stosowane wkładki i moduły muszą być wspierane przez producenta urządzeń i być objęte możliwością analizy potencjalnych błędów w trakcie potencjalnych zgłoszeń serwisowych. Wkładki i moduły muszą pochodzić z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej
   5) Wszystkie urządzenia dostarczone i zastosowane przez Wykonawcę będą pochodziły z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej. Spełnienie powyższego wymogu zostanie potwierdzone oświadczeniem producenta Urządzeń lub jego polskiego przedstawicielstwa, które Wykonawca zobowiązuje się dostarczyć Zamawiającemu najpóźniej w dniu dostawy oferowanych Urządzeń
   6) Wykonawca dostarczy, na etapie dostawy pakietów serwisowych, pisemne oświadczenie wystawione przez producenta lub Wykonawcę, że dostarczane pakiety serwisowe są dedykowane do zaoferowanych przez Wykonawcę aktywnych Urządzeń sieciowych i oprogramowania.
   7) Gwarancja będzie liczona od daty odbioru przedmiotu umowy i oparta na gwarancji producentów rozwiązania, jednak nie krótsza niż 36 miesięcy.
   8) Serwis gwarancyjny świadczony ma być w miejscu instalacji Urządzeń.
   9) Gwarancja ma być świadczona w reżimie 24x7x4, gdzie 24 godz. to czas naprawy Awarii, 4 godz. to czas reakcji przez 7 dni w tygodniu. Czas naprawy Awarii liczony jest od czasu przesłania zgłoszenia o awarii do Wykonawcy zgodnie z procedurą przyjmowania zgłoszeń serwisowych
   10) Zamawiający wymaga by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części oryginalne zgodnie z metodyką i zaleceniami producenta. Spełnienie powyższego wymogu zostanie potwierdzone odpowiednim oświadczeniem Wykonawcy, potwierdzonym przez producenta Urzadzeń (lub jego polskiego przedstawicielstwa)
   11) Zamawiający wymaga by dostarczone Oprogramowanie było Oprogramowaniem w wersji najnowszej, dostępnej na rynku dla zaproponowanych urządzeń w terminie co najmniej 21 dni przed terminem składania oferty
   12) Wykonawca zobowiązany jest do dostarczania poprawek do Oprogramowania w ramach dostarczanych licencji w okresie trwania wsparcia serwisowego.
   13) Oferowane urządzenia nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży

14) Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego
15) Zamawiający zastrzega sobie prawo do dodawania nowych modułów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą
16) W okresie gwarancji Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania do najnowszych wersji oferowanych przez producenta (włączając tzw. firmware) oraz patche i programy korekcji błędów, a także dostęp do usług wsparcia technicznego producenta właściwy dla danego Urządzenia lub Oprogramowania. W przypadku, gdy dostęp taki wymaga podania nazwy użytkownika, hasła lub numeru seryjnego Wykonawca dostarczy Zamawiającemu ww. przed podpisaniem protokołu odbioru Urządzeń.
17) W przypadku konieczności naprawy Urządzenia lub Oprogramowania poza Lokalizacją, Wykonawca zorganizuje transport do miejsca naprawy oraz po naprawie do Lokalizacji użytkowania oraz pokrywa jego koszty i ponosi ryzyko uszkodzenia lub przypadkowej utraty Urządzenia lub Oprogramowania Standardowego
18) W przypadku awarii lub dostarczenia dysku twardego jako rozwiązania równoważnego albo zastosowania dysku twardego jako rozwiązania zastępczego będzie on wymieniony przez Wykonawcę na nowy dysk twardy o nie gorszych parametrach technicznych bez konieczności zwrotu uszkodzonego dysku twardego i dokonywania ekspertyzy poza siedzibą Użytkownika. Dyski twarde użyte przez Wykonawcę w sytuacjach, o których mowa w zdaniu poprzedzającym mogą być używane przez Wykonawcę pod warunkiem, że nie opuszczą lokalizacji Zamawiającego.
19) Na okres przedłużającej się naprawy Wykonawca może stosować procedury zastępcze. Czas trwania procedur zastępczych nie może być dłuższy niż 45 dni kalendarzowych od chwili zgłoszenia awarii
20) Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności Systemu we wszystkich modułach i zaprzestanie stosowania w bieżącej pracy rezerwowego Urządzenia i/lub procedur zastępczych
21) Po usunięciu każdej Awarii, Wykonawca zobowiązuje się do doprowadzenia całego systemu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów
22) Wykonawca do dostarczonego Urządzenia, będącego przedmiotem zamówienia, dołączy karty gwarancyjne zawierające numer seryjny, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne Wykonawca w terminie 7 dni od zawarcia Umowy dostarczy Zamawiającemu (do akceptacji i stosowania) procedury zgłaszania i obsługi Awarii wraz z listą osób upoważnionych do kontaktów, wykazem adresów poczty elektronicznej, nr telefonów i nr faksów
23) Wykonawca, najpóźniej w dniu zawarcia Umowy, przedstawi do akceptacji Zamawiającemu listę osób uprawnionych do wykonywania czynności serwisowych
24) W okresie gwarancji Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie urządzeń i oprogramowania stanowiącego przedmiot zamówienia
25) Wymagany tryb zgłaszania wszelkich awarii i błędów. Zgłoszenie następuje w drodze pisemnej faksem lub mailem na adres podany przez Wykonawcę:

fax pod numer .....
e-mail na adres .....

26) Usługa świadczona w okresie gwarancji przez Wykonawcę na rzecz Zamawiającego, polegająca m.in. na telefonicznym, faksowym lub za pośrednictwem poczty elektronicznej udzielaniu informacji związanych z funkcjonalnością i obsługą Systemu, a także rozwiązywaniu doraźnych problemów w ramach funkcjonowania Systemu.

10. Wymagania w zakresie warunków redundancji

Redundancja dla dostarczanych urządzeń musi uwzględniać poziom nadmiarowości dla budowanego systemu rzędu N+1 zgodnie z normą TIA-942 (lub równoważną), która określa nadmiarowość w postaci jednego dodatkowego urządzenia, modułu, ścieżki lub systemu ponad minimum określone wymaganiami podstawowymi. Uszkodzenie lub konserwacja jednego z dwóch urządzeń, modułów lub ścieżek nie spowoduje przerwy w pracy systemu.

11. Warunki i zakres wdrożenia

11.1. Zakres prac do wykonania w ramach dostawy rozwiązania z punktu 6.5

Zamawiający wymaga:

1. Opracowania w porozumieniu z Zamawiającym dokumentacji projektowej, a w szczególności:
    a. profili konfiguracyjnych dla urządzeń sieciowych Zamawiającego będących na ścieżce przesyłu danych (integracja z systemem):
        i. Routery Cisco serii ASR 3800, 3900
        ii. Switche Cisco Nexus 7k oraz Catalyst 6800
        iii. Switche Cisco Catalyst 6500 wraz z zainstalowanym modułem ACE30
        iv. Switche Cisco 3650
        v. Switche Juniper EX
        vi. Firewalle Juniper SRX
        vii. Firewalle Checkpoint
        viii. Firewalle sieciowe Cisco ASA
2. Opracowania zakresu oraz harmonogramu wdrożenia we współpracy z Zamawiającym.
3. Uruchomienia dedykowanych platform sprzętowych, instalacji dostarczonego oprogramowania zarówno na platformach sprzętowych jak i z wykorzystaniem maszyn wirtualnych dostarczanych zgodnie z punktem 6.7.
4. Konfiguracji poszczególnych elementów, tak aby rozwiązanie spełniało funkcjonalność jednolitego systemu
5. Wdrożenie systemu polegać będzie na:
    a. fizycznej instalacji serwerów fizycznych w serwerowniach Zamawiającego
    b. dokonaniu konfiguracji zainstalowanych urządzeń i oprogramowania zgodnie z dokumentacją projektową uwzględniajacą integrację z istniejącą infrastruktura Zamawiającego
    c. optymalizacji konfiguracji urządzeń oraz systemów wdrożonych w ramach niniejszego projektu z usługami działającymi w infrastrukturze sieciowej Zamawiającego
    d. bieżącej analizie i administrowaniu nowowdrożonymi systemami
    e. analizie danych na bieżąco spływających do wdrożonego systemu, konfigurowanie zmian wynikających z tej analizy, w tym generowanie raportów ze

współpracujących ze sobą nowowdrożonych systemów na zlecenie administratorów.

6. Wdrożenie systemu zgodnie z opracowaną dokumentacją projektową.
7. Integracji z Systemem uwierzytelniania pracującym z użyciem protokołu 802.1x, będącym przedmiotem zamówienia.
8. Opracowania dokumentacji powykonawczej. Wszelkie odstępstwa od dokumentacji projektowej powinny zostać zawarte w dokumentacji powykonawczej.

11.2. Zakres prac do wykonania w ramach dostawy rozwiązania z punktu 6.6:

Zamawiający wymaga:

1. Opracowania w porozumieniu z Zamawiającym dokumentacji projektowej, a w szczególności:
    2. polityk dostępowych
    3. plików konfiguracyjnych dla wszystkich urządzeń Zamawiającego objętych zakresem wdrożenia systemu kontroli dostępu
    4. polityk głębokiej analizy systemu stacji końcowej
    5. w przypadku użycia dodatkowych modułów wymagających instalacji na stacjach końcowych, Zamawiający wymaga opracowania dokumentacji zawierającej procedurę instalacji danych elementów przez Administratorów systemów stacji końcowych
    6. wykorzystania istniejącego PKI w procesie uwierzytelnienia (w przypadku niekompatybilności rozwiązania Zamawiający dopuszcza uruchomienie przez Wykonawcę dodatkowego systemu PKI na koszt Wykonawcy)
    7. integracji z zewnętrznym działającym systemem LDAP będącym na wyposażeniu Zamawiającego
    8. planu migracji z aktualnie użytkowanego systemu CS-ACS
2. Opracowania zakresu oraz harmonogramu wdrożenia we współpracy z Zamawiającym
3. Konfiguracji poszczególnych elementów, tak aby rozwiązanie spełniało funkcjonalność jednolitego systemu
4. Wdrożenie systemu polegać będzie na:
    a. fizycznej instalacji serwerów fizycznych w serwerowniach Zamawiającego
    b. instalacji dostarczonego oprogramowania zarówno na platformach sprzętowych jak i z wykorzystaniem maszyn wirtualnych dostarczanych zgodnie z punktem 6.7 oraz urządzeń dostarczonych w ramach punktu 6.6
    c. dokonaniu konfiguracji zainstalowanych urządzeń i oprogramowania zgodnie z dokumentacją projektową uwzględniającą integrację z istniejącą infrastruktura Zamawiającego
    d. optymalizacji konfiguracji urządzeń oraz systemów wdrożonych w ramach niniejszego projektu z usługami działającymi w infrastrukturze sieciowej Zamawiającego
    e. bieżącej analizie i administrowaniu nowowdrożonymi systemami
    f. analizie danych na bieżąco spływających do wdrożonego systemu, konfigurowanie zmian wynikających z tej analizy, w tym generowanie raportów ze współpracujących ze sobą nowowdrożonych systemów na zlecenie administratorów.
5. Wdrożenie systemu zgodnie z opracowaną dokumentacją projektową.
6. Integracji z system telemetrii sieciowej, wykrywania zagrożeń i ataków będącym przedmiotem zamówienia.

7. Opracowania dokumentacji powykonawczej. Wszelkie odstępstwa od dokumentacji projektowej powinny zostać zawarte w dokumentacji powykonawczej.

11.3. Zakres prac do wykonania w ramach dostawy urządzeń z punktu 6.1

Zamawiający wymaga:

1. dostarczenie dwunastu przełączników z punktu 6.1 według specyfikacji określonej przez Zamawiającego.
2. transport, rozładunek, wniesienie sprzętu do pomieszczeń wskazanych przez Zamawiającego
3. instalację przełączników w zakresie:
    a. fizycznej instalacji w szafach w sześciu punktach dystrybucji w miejscu wskazanym przez Zamawiającego
    b. uruchomienia urządzeń z oprogramowaniem rekomendowanym przez producenta
    c. konfiguracji urządzeń. Przełączniki mają zastąpić dwanaście obecnie pracujących przełączników serii Cisco 3550, 3560. Konfiguracja nowych przełączników powinna zapewnić zachowanie obecnej funkcjonalności przełączników Cisco serii 3500. Ewentualne zmiany w konfiguracji mogą wynikać z potrzeby migracji na nowszą wersję oprogramowania, potrzeby połączenia urządzeń w „stack", zintegrowanie urządzeń do systemu NAC (dotyczy rozwiązania z punktu 6.6) oraz systemów obecnie zintegrowanych z dotychczasowymi przełącznikami.
    d. podłączenie (okablowanie) przełączników do infrastruktury Klienta. Zamawiający dopuszcza wykorzystanie istniejącego obecne okablowania tam, gdzie jest to możliwe i nie spowoduje obniżenia wydajności urządzeń.
    e. deinstalacja obecnie pracujących dwunastu przełączników
    f. sporządzenie powykonawczej dokumentacji technicznej. Wszelkie odstępstwa od dokumentacji projektowej powinny zostać zawarte w dokumentacji powykonawczej.

11.4. Zakres prac do wykonania w ramach dostawy urządzeń z punktu 6.2

Zamawiający wymaga:

1. dostarczenie ośmiu routerów opisanych w punkcie 6.2 według specyfikacji określonej przez Zamawiającego.
2. transport, rozładunek, wniesienie sprzętu do pomieszczeń wskazanych przez Zamawiającego
3. instalację routerów w zakresie:
    a. fizycznej instalacji w szafach, w miejscu wskazanym przez Zamawiającego (dwie lokalizacje na terenie Warszawy)
    b. uruchomienia urządzeń z oprogramowaniem rekomendowanym przez producenta
    c. konfiguracji urządzeń zgodnie z dokumentacją projektową. Nowe routery mają zastąpić osiem obecnie pracujących routerów serii Cisco 3800. Konfiguracja nowych routerów powinna zapewnić zachowanie obecnej funkcjonalności dostarczanej przez routery Cisco 3825. Ewentualne zmiany w konfiguracji mogą wynikać z potrzeby migracji z systemu operacyjnego IOS na nowy system operacyjny dostarczany z routerami.
4. podłączenie (okablowanie) routerów do infrastruktury Klienta. Zamawiający dopuszcza wykorzystanie istniejącego obecne okablowania tam, gdzie jest to możliwe i nie spowoduje obniżenia wydajności urządzeń.

5. deinstalacja obecnie pracujących ośmiu routerów Cisco 3825
6. opracowanie dokumentacji technicznej powykonawczej. Wszelkie odstępstwa od dokumentacji projektowej powinny zostać zawarte w dokumentacji powykonawczej.

11.5. Zakres prac do wykonania w ramach dostawy urządzeń z punktu 6.3

Zamawiający wymaga:

1. dostarczenie ośmiu urządzeń z punktu 6.3 według specyfikacji określonej przez Zamawiającego.
2. transport, rozładunek, wniesienie sprzętu do pomieszczeń wskazanych przez Zamawiającego
3. Instalację urządzeń w zakresie:
    a. fizycznej instalacji w szafach, w miejscu wskazanym przez Zamawiającego (2 lokalizacje na terenie Warszawy)
    b. uruchomienia urządzeń z oprogramowaniem rekomendowanym przez producenta
    c. konfiguracji urządzeń. Urządzenia mają zastąpić obecnie pracujące urządzenia Cisco ASA 5520. Konfiguracja urządzeń powinna zapewnić zachowanie obecnej funkcjonalności dostarczanej przez urządzenia ASA 5520. Ewentualne zmiany w konfiguracji mogą wynikać z potrzeby migracji na nowszą wersję oprogramowania itp.
    d. przeniesienie obecnych polityk bezpieczeństwa
    e. uruchomienia urządzeń w klastrach active - active
    f. Uruchomienia funkcjonalności modułu wykrywania i zapobiegania włamań.
    g. Opracowania polityki bezpieczeństwa. Analizy otrzymanych zdarzeń oraz optymalizację reguł w celu lepszej ochrony środowiska Zamawiającego.
    h. Instalacji i uruchomienia systemu zarządzającego dla modułów wykrywania i zapobiegania włamań z punktu 6.4.
    i. podłączenia (okablowanie) urządzeń do infrastruktury Klienta. Zamawiający dopuszcza wykorzystanie istniejącego obecne okablowania tam, gdzie jest to możliwe i nie spowoduje obniżenia wydajności urządzeń.
    j. deinstalację obecnie pracujących dwóch urządzeń Cisco ASA 5520
    k. sporządzenie powykonawczej dokumentacji technicznej. Wszelkie odstępstwa od dokumentacji projektowej powinny zostać zawarte w dokumentacji powykonawczej.

11.6. Zakres prac do wykonania w ramach dostawy rozwiązania z punktu 6.7

Zamawiający wymaga:

1. dostarczenie serwerów według specyfikacji określonej przez Zamawiającego.
2. transport, rozładunek, wniesienie sprzętu do pomieszczeń wskazanych przez Zamawiającego
3. Instalację urządzeń w zakresie:
    a. fizycznej instalacji w serwerów w szafach, w miejscu wskazanym przez Zamawiającego (2 lokalizacje na terenie Warszawy)
    b. podłączenia urządzeń do zasilania
    c. poprowadzenie okablowania pomiędzy wdrażanymi urządzeniami
    d. uruchomienie i konfiguracja urządzeń
    e. instalacja systemu zarządzającego serwerami hiperkonwergentnymi i oprogramowaniem wirtualizującym.
    f. integracja z systemami dostarczonymi w ramach punktu 6.5 oraz punktu 6.6

g. integracja logiczna dwóch DC
h. konfiguracja systemu Backupu opisanego w punkcie 6.7.1 oraz 6.7.1.1

4. Wykonania dokumentacji powykonawczej. Wszelkie odstępstwa od dokumentacji projektowej powinny zostać zawarte w dokumentacji powykonawczej.

11.7. Zakres prac do wykonania w ramach punktu 6.10

Zamawiający wymaga:

1. dostarczenie firewalli według specyfikacji określonej przez Zamawiającego.
2. transport, rozładunek, wniesienie sprzętu do pomieszczeń wskazanych przez Zamawiającego
3. Opracowania w porozumieniu z Zamawiającym dokumentacji projektowej, a w szczególności:
   a. plików konfiguracyjnych dla wszystkich urządzeń Zamawiającego objętych zakresem wdrożenia
   b. planu migracji z aktualnie użytkowanego urządzenia ASA5585X
4. Opracowania zakresu oraz harmonogramu wdrożenia we współpracy z Zamawiającym
5. Konfiguracji poszczególnych elementów, tak aby rozwiązanie spełniało funkcjonalność dostarczaną przez aktualnie wykorzystywane urządzenie ASA5585X. Ewentualne zmiany w konfiguracji mogą wynikać z potrzeby migracji na nowszą wersję oprogramowania itp.
6. Wdrożenie systemu polegać będzie na:
   a. fizycznej instalacji zaoferowanych urządzeń w serwerowniach Zamawiającego
   b. instalacji dostarczonego oprogramowania zarówno na platformach sprzętowych jak i z wykorzystaniem maszyn wirtualnych
   c. dokonaniu konfiguracji zainstalowanych urządzeń i oprogramowania zgodnie z dokumentacją projektową uwzględniającą integrację z istniejącą infrastruktura Zamawiającego
   d. optymalizacji konfiguracji urządzeń
   e. przeniesienie obecnych polityk bezpieczeństwa
   f. uruchomienia urządzeń w klastrach
   g. Uruchomienia funkcjonalności modułu wykrywania i zapobiegania włamań.
7. Opracowania polityki bezpieczeństwa i analizy otrzymanych zdarzeń oraz optymalizację reguł w celu lepszej ochrony środowiska Zamawiającego.
8. Instalacji i uruchomienia systemu zarządzającego dostarczonego w ramach punktu 6.4.
9. podłączenia (okablowanie) urządzeń do infrastruktury Klienta. Zamawiający dopuszcza wykorzystanie istniejącego obecne okablowania tam, gdzie jest to możliwe i nie spowoduje obniżenia wydajności urządzeń.
10. Opracowania dokumentacji powykonawczej. Wszelkie odstępstwa od dokumentacji projektowej powinny zostać zawarte w dokumentacji powykonawczej.

12. Wymagania szczegółowe

1. Wszelkie wymagania wskazane w niniejszym dokumencie należy traktować jako wymagania minimalne
2. Prace obejmują w szczególności:
   a. Dostarczenie Urządzeń do wskazanych przez Zamawiającego Lokalizacji;
   b. Rozpakowanie Urządzeń oraz utylizacja/magazynowanie opakowań;
   c. Montaż Urządzeń w szafach typu rack 19";

d. Podłączenie Urządzeń do zapewnianych przez Zamawiającego obwodów zasilających i sieci komputerowych;
e. Konfiguracja sprzętowa Urządzeń;
f. Uruchomienie Urządzeń;
g. Update Oprogramowania sprzętowego;

3. Usługi obejmują w szczególności:
   a. rekonfigurację Infrastruktury w celu integracji z Urządzeniami i Oprogramowaniem oraz podniesieniem bezpieczeństwa i niezawodności Systemu w zakresie dołączenia przełączników sieci LAN do warstwy rdzeniowej Datacenter uwzględniająca wysoką dostępność, niezawodność, minimalizację opóźnień przełączenia oraz wysoką zbieżność sieci w razie awarii,
   b. dołączenie nowodostarczonych urządzeń do systemów zarządzających pracujących w infrastrukturze Zamawiającego,
   c. przeniesienie systemów zarządzających pracujących w infrastrukturze Zamawiającego na urządzenia dostarczane zgodnie z opisem w punkcie 6.7
   d. W ramach reorganizacji należy uwzględnić protokoły pracujące w obecnej sieci i planowane wdrożenie powinno uwzględniać dostarczenie podobnej funkcjonalności do wykorzystywanych protokołów.
   e. Implementacja obecnych polityk bezpieczeństwa na dostarczonych zaporach ogniowych. W szczególności na urządzeniach tych będą uruchomione funkcjonalności gwarantujące:
   f. analizę i inspekcje ruchu w tym z wykorzystaniem modułów IPS i personalizowanych sygnatur (zgodnie z przygotowanym projektem technicznym);
   g. redundantne połączenia zapór ogniowych w warstwie fizycznej;
   h. mechanizmy redundancji działania zapory ogniowej;
   i. kształtowanie parametrów synchronizacji;
   j. wirtualizacje mechanizmów zapór ogniowych;
   k. W ramach projektu technicznego Wykonawca zaproponuje plan i scenariusze testów akceptacyjnych uwzględniających implementowane rozwiązania i wdrażane urządzenia.
   l. W ramach usługi wdrożeniowej opisanej w punkcie 3 Wykonawca przeprowadzi testy akceptacyjne zgodnie z projektem technicznym.
   m. Wykonawca zainstaluje dostarczony sprzęt w szafach posiadanych przez Zamawiającego (42U 800mmx1000mm). Wykonawca dostarczy odpowiednią ilość listew zasilających do podłączenia dostarczanych urządzeń, kabli krosujących Optycznych oraz miedzianych niezbędnych do zainstalowania całego środowiska.
   n. Dla urządzeń opisanych w punkcie 6.1 Zamawiający oczekuje dostarczenia następującego okablowania światłowodowego: Patchcord światłowodowy multimode 2 metry SC-LC – 12 szt.
   o. Wykonawca dokona fizycznej instalacji wszystkich urządzeń zgodnie z wcześniej opracowanym projektem technicznym w miejscach uzgodnionych wspólnie z Zamawiającym
   p. Rekonfiguracja CISCO Prime Infrastructure 3.1, Cisco LMS 4.2.5, CSM, DCMN, Cisco Firepower Management Center obejmująca dołożenie nowo dostarczanych urządzeń.

q. Konfiguracja oprogramowania syslog do zbierania zdarzeń z wszystkich urządzeń aktywnych w infrastrukturze sieciowej Zamawiającego na dostarczanym rozwiązaniu opisanym w punkcie 6.7.
r. Przeniesienie systemów zarządzających Zamawiającego (CISCO Prime Infrastructure 3.1, Cisco LMS 4.2.5, CSM, DCMN, Cisco Firepower Management Center, Dashboard CheckPoint, Junos Space, McAfee NSM, Tuffin) oraz systemów operacyjnych Linux RedHat 6.6, Windows Server 2012, Windows Server 2008 na dostarczone przez Wykonawcę środowisko wirtualne opisane w punkcie 6.7.
s. Instalacja dostarczonych systemów i oprogramowania na środowisku wirtualnym opisanym w punkcie 6.7.

13. Wymagania w zakresie przeprowadzenia instruktażu wdrożeniowego

1) Wykonawca w ramach realizacji całości projektu przeprowadzi instruktaż wdrożeniowy dotyczący urządzeń i oprogramowania opisanych w punktach 6.5 oraz 6.6 oraz 6.7.
2) Instruktaż wdrożeniowy powinien zostać zrealizowany w siedzibie zamawiającego. Dopuszczana jest realizacja instruktażu wdrożeniowego poza siedzibą Zamawiającego; wówczas Wykonawca poniesie koszty akomodacji i wyżywienia, jak również zapewni zaplecze techniczno-dydaktyczne oraz zorganizuje instruktaż w dwóch turach w różnym okresie czasu.
3) Instruktaż musi być przeprowadzony w języku polskim, a materiały instruktażowe powinny być dostarczone w języku polskim lub angielskim.
4) Wykonawca opracuje harmonogram instruktażu zawierający:
   a) cel i projektowany zakres instruktażu,
   b) informacje o zakresie tematycznym instruktażu,
   c) metodę i formę instruktażu,
   d) czas trwania instruktażu
5) Harmonogram, o którym mowa w pkt. 4). Wykonawca przedstawi do akceptacji Zamawiającego w terminie 10 Dni Roboczych przed rozpoczęciem danego rodzaju instruktażu.
6) Instruktaż powinien być przeprowadzony dwóm zespołom tj. zespół administratorów sieci – 5 osób oraz zespół administratorów stacji końcowych – 3 osoby.
7) W przypadku odbycia się instruktażu poza siedzibą zamawiającego wymagane jest, aby w jednej turze instruktażu wzięło udział minimum dwóch administratorów sieci.
8) Instruktaż musi być realizowany przez przedstawicieli Wykonawcy z zastosowanych rozwiązań technicznych i obejmować wprowadzenie teoretyczne oraz praktyczne.
9) W przypadku instruktażu wdrożeniowego przeprowadzonego z rozwiązania opisanego w punkcie 6.5 Zamawiający wymaga, aby odbył się w wymiarze 24 godzin z zakresu konfiguracji, administracji i monitoringu budowanego rozwiązania wyłącznie dla zespołu administratorów sieci.
10) W przypadku instruktażu wdrożeniowego przeprowadzonego z rozwiązania opisanego w punkcie 6.6 Zamawiający wymaga, aby odbył się w wymiarze 40 godzin z zakresu konfiguracji, administracji i monitoringu budowanego rozwiązania dla zespołu administratorów sieci oraz 24 godzin z zakresu obsługi stanowisk końcowych dla zespołu administratorów stacji końcowych.

11) W przypadku instruktażu wdrożeniowego przeprowadzonego z rozwiązania opisanego w punkcie 6.7 Zamawiający wymaga, aby odbył się w wymiarze 40 godzin z zakresu konfiguracji, administracji i monitoringu budowanego rozwiązania wyłącznie dla zespołu administratorów sieci.

14. Wymagania w Zakresie Dokumentacji

Wykonawca w ramach realizacji przedmiotu zamówienia dostarczy dokumentację spełniającą wymagania określone poniżej:

1. Zamawiający wymaga, aby Wykonawca przygotował, zgodnie z ogólnie akceptowalnymi standardami w dziedzinie dokumentowania, następujące rodzaje Dokumentacji bezpośrednio związanej z przedmiotem zamówienia:
    a. Projekt Techniczny wykonany zgodnie z Wymaganiami Dotyczącymi Usług Dodatkowych opisanych w pkt. 6, zawierający Plan Wdrożenia
    b. Dokumentację Powykonawczą (dot. dostawy Urządzeń oraz Usług)
    c. Dokumentację Eksploatacyjną
    d. Plan Zarządzania Projektem, zawierający co najmniej obszary:
        i. Organizacja Projektu,
        ii. Plan komunikacji
        iii. Harmonogram Projektu
        iv. Plan Zarządzania Jakością
        v. Plan Zarządzania Ryzykiem
        vi. Plan Zarządzania Zagadnieniami
        vii. Produkty Projektu
    e. Plan i opis realizacji instruktarzu wdrożeniowego
    f. Wykaz Ilościowo-Cenowy dostarczonych produktów, który stanowi załącznik do faktury.
2. Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji przedsięwzięcia charakteryzowały się wysoką jakością, na którą będą miały wpływ takie czynniki jak:
    a. Struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób.
    b. Zachowanie standardów, w tym notacji UML, a także sposób pisania, rozumianych jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu.
    c. Zachowanie standardów Zamawiającego w zakresie oznaczeń dokumentów, wersjonowania, metryk,
    d. Kompletność dokumentu rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia.
    e. Spójność i niesprzeczność dokumentu rozumiane jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.
3. Wymagane jest, aby w ramach Dokumentacji Wykonawca przekazał Zamawiającemu pliki źródłowe zastosowanych w niej obrazów, w tym m.in. schematów, rysunków, topologii oraz wykresów, w formacie niezabezpieczonym i edytowalnym.
4. Wymagane jest, aby w ramach Dokumentacji Wykonawca przekazał Zamawiającemu wszystkie dokumenty robocze wytworzone w takcie realizacji niniejszego

zamówienia, w szczególności analizy, arkusze kalkulacyjne, materiały robocze, w formacie elektronicznym, niezabezpieczonym i edytowalnym.

5. Wszystkie Dokumenty przekazane w formie elektronicznej (pliki) muszą:
   a. być posegregowane w folderach odpowiadających nazwą produktów oraz nazwą, wersją i podwersją przekazywanego modułu (dotyczy kodów źródłowych),
   b. być posegregowane w folderach zgodnie ze strukturą Dokumentacji,
   c. posiadać nazwy plików (razem ze ścieżką) krótsze niż 200 znaków,
6. W przypadku kolejnych wersji Dokumentacji wymagane jest, aby Wykonawca dostarczał elektroniczne wersje Dokumentacji, które zawierają wyróżnione różnice pomiędzy kolejnymi wersjami Dokumentacji (w trybie rejestracji zmian).
7. Wykonawca przedstawi do akceptacji Zamawiającego dokument „Dokumentacja Powykonawcza (dot. dostawy Urządzeń i rozwiązań)", zawierający co najmniej przebieg (wraz ze szczegółowym opisem) prac oraz opis czynności wdrożeniowych (w tym napotkanych problemów wraz z opisem ich rozwiązania).
8. Wykonawca Umowy dostarczy Zamawiającemu Wykaz Ilościowo-Cenowy przedmiotu zamówienia z podziałem na:
   a. Urządzenia – wykazanie każdego Urządzenia, wraz ze specyfikacją podzespołów,
   b. Oprogramowanie – wykazanie każdego rodzaju Oprogramowania,
   c. Wartości niematerialne i prawne – wykazanie licencji Oprogramowania Standardowego i autorskich praw majątkowych do wytworzonej Dokumentacji.
9. Poza powyższym Wykaz Ilościowo-Cenowy powinien zawierać podział na:
   a. nazwę ,
   b. producenta,
   c. numer seryjny,
   d. kod produktu/model,
   e. opis,
   f. ilość,
   g. lokalizacja instalacji,
   h. cena jednostkowa brutto w PLN,
   i. cena jednostkowa netto w PLN,
   j. wartość brutto w PLN.
10. Wykonawca do Dokumentacji dołączy wykaz zawierający szczegółowy spis Dokumentów wraz z opisem ich przeznaczenia.
11. Wykonawca dostarczy instrukcję postępowania w dostępie do wdrożonej struktury sieci LAN dla użytkownika końcowego (stacji końcowej).

15. Wymagania w zakresie zgodności z przepisami prawa

1. Rozwiązanie dla Systemu musi być zgodne z niżej wymienionymi aktami prawnymi:
   a. Ustawa o ochronie danych osobowych z dnia 29.08.1997 roku. (t.j. Dz. U. z 20.06.2016r. poz. 922);
   b. Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12.04.2012 r. (t.j. z 25.01.2016r. poz. 113 z późn.zm.) ;

c. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17.02.2005 roku (tekst jednolity Dz. U. z 22.08.2014 r., poz. 1114 z późn.zm.);
d. Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (t.j. Dz. U. z 17.02.2016r., poz. 191 z późn. zm.);
e. Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. Dz. U. z 18.03.2014 r. poz. 333, z późn. zm.);
f. Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (t.j. Dz. U. z 16.09.2016r., poz. 1489 z późn.zm.);
g. Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (t.j. Dz. U. z 18.11.2016r., poz. 1868, z późn. zm.);
h. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jednolity Dz. U. z 02.10.2013 r., poz. 1166 z późn. zm.);
i. Ustawa z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (Dz. U. z 23.12.2013 poz. 1635 z późn. zm.);
j. Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej) - Dz.U.UE.L.2002.108.51 z późn. zm.;

k. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 grudnia 2015r. w sprawie centralnego punktu systemu centrów powiadamiania ratunkowego oraz punktów centralnych służb (Dz. U. z 31.12.2015r. poz. 2356)

2. Wykonawca dostarczy sprzęt fabrycznie nowy (tzn. wyprodukowany nie dawniej niż na 6 miesięcy przed ich dostarczeniem), wolny od wad technicznych i prawnych, dopuszczony do obrotu na terenie Polski oraz Unii Europejskiej, dobrej jakości. Sprzęt nie może być używany w żadnych innych projektach. Nie dopuszcza się urządzeń odnowionych tzw. refubrished (zwróconych do producenta i później odsprzedawanych ponownie przez producenta). Zamawiający wymaga dostarczenia przez Wykonawcę wraz z dostawą sprzętu oświadczenia od Producenta informującego o dacie produkcji (kwartał / miesiąc)
3. Zamawiający wymaga, aby dostarczone urządzenia pochodziły z autoryzowanego kanału sprzedaży producentów urządzeń na rynek polski lub Unii Europejskiej. . Zamawiający będzie żądał stosownego potwierdzenia podpisanego przez polskie biuro przedstawiciela producenta. Jeśli producent nie posiada oficjalnego biura w Polsce przez przedstawiciela biura europejskiego, odpowiadającego za rynek polski. Potwierdzenie Wykonawca zobowiązany jest dostarczyć Zamawiającemu wraz z dostawą sprzętu.
4. W przypadku braku takiego potwierdzenia, Zamawiający ma prawo odmówić przyjęcia takiego sprzętu i wyznaczyć Wykonawcy dodatkowy termin na przedłożenie takiego potwierdzenia. Po bezskutecznym upływie tego terminu Zamawiający będzie miał prawo do odstąpienia od umowy ze skutkiem natychmiastowym i żądania kary umownej w wysokości określonej w istotnych postanowieniach umowy (wzorze umowy).
5. Zamawiający musi posiadać pełne prawa do korzystania z dostarczonych licencji i oprogramowania. Dostarczony towar musi być wolny od wad prawnych, nie mogą mieć do niego prawa osoby trzecie oraz nie może być przedmiotem żadnego postępowania ani zabezpieczenia.

6. Zamawiający wymaga, aby wraz z dostawą sprzętu Wykonawca przedstawił na życzenie Zamawiającego oficjalne potwierdzenie wykupienia kontraktów serwisowych u Producenta na urządzenia zgodnie z SIWZ na cały okres gwarancji.