Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Specyfikacja Techniczna – załącznik nr 9 do SWZ:

„Dostawa i wdrożenie sprzętu informatycznego w ramach konkursu grantowego „Cyfrowa Gmina”

Spis treści

Wstęp

W ramach zadania wykonawca dostarczy sprzęty i oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia zgodnego z opisem w sekcji „Wdrożenie".
Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

a) Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
b) Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane
c) Sprzęt musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;
d) Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
e) Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
f) Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:
    i. połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
    ii. łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
    iii. zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
    iv. wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,
    v. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50Hz;

System Firewall (1 komplet)

1. Zapora sieciowa typu Next Generation Firewall (NGFW),
2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku.
3. Minimalna ilość interfejsów:
    a) 6 interfejsów 10 GbE SFP+,
    b) 4 interfejsy 5 GbE SFP+,

c) 24 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.
d) 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G,
e) 1 interfejs konsoli do zarządzania zaporą,
f) 1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą,

4. Zapora powinna posiadać dysk M.2 o pojemności przynajmniej 64 GB z możliwością wymiany na większy.
5. Urządzenie musi posiadać min. dwa zasilacze.
6. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa
7. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji,
8. Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q,
9. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej,
10. Minimalna ilość jednocześnie obsługiwanych połączeń: 1 900 000,
11. Możliwość obsłużenia przynajmniej 22 000 nowych połączeń w ciągu 1 sekundy.
12. Przepustowość urządzenia pracującego w trybie stateful firewall: min. 5,1 Gbps – dla ramki 1518B zgodnie z RFC 2544,
13. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: min. 3.7 Gbps,
14. Przepustowość urządzenia pracującego jako koncentrator VPN: min. 2,2 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544,
15. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – min. 3,4 Gbps,
16. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 2 500,
17. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: min. 2 z możliwością rozszerzenia do przynajmniej 500
18. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: min. 50 z możliwością rozszerzenia do przynajmniej 1 000.
19. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.
20. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 850 Mbps oraz obsłużyć min. 150 000 połączeń.
21. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP,
22. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site),

23. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa),
24. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP,
25. Wsparcie dla Dynamicznego DNS tzw. DDNS,
26. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.
27. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).
28. Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:
    a) wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),
    b) wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,
    c) wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.
29. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps,
30. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.
31. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.
32. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.
33. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN),
34. Kontrola dostępności zestawionych tuneli VPN,
35. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.
36. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.
37. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić),
38. Funkcja NAT oparta o reguły bezpieczeństwa.

39. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe),
40. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
41. Zintegrowany system skanowania antyspyware,
42. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.
43. System IPS musi używać algorytmu szeregowego przetwarzania.
44. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
45. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji,
    a) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.
    b) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur,
    c) Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.
46. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
47. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa,
48. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi,
49. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p,
50. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń
51. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
52. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss.
53. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
54. Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 32 takich punktów dostępowych sieci bezprzewodowej.
55. **Wymagane jest dostarczenie dodatkowego urządzenia pełniącego funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym. Urządzenie standby powinno mieć identyczne parametry wydajnościowe oraz sprzętowe jak podstawowa jednostka. Urządzenia powinny synchronizować pomiędzy sobą stany sesji połączeń**.

56. Gwarancja: Min. 36 mc, wsparcie w trybie 24x7.
57. Wymagane licencje:
    a) Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 3 lata.

Przełącznik sieciowy ISCSI (2sztuki)

1. Przełącznik posiadający min. 16 portów 10Gigabit Ethernet SFP+, mogących pracować z prędkością 100 MB, 1G lub 10G lub wyżej – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+
2. Wysokość urządzenia 1U
3. Przełącznik musi posiadać redundancję systemu zasilania poprzez min. dwa wewnętrzne zasilacze.
4. Przełącznik musi mieć możliwość montażu zasilaczy AC lub DC w zależności od potrzeb
5. Przełącznik musi posiadać możliwość instalacji zestawu wentylatorów zapewniających chłodzenie przód-tył, lub tył-przód.
6. Zarówno zasilacze jak i wentylatory muszą mieć możliwość wymiany podczas pracy urządzenia (hot-swap)
7. Nieblokująca architektura o wydajności przełączania min. 320 Gb/s
8. Szybkość przełączania min. 238 Milionów pakietów na sekundę
9. Średnie opóźnienia na portach maksimum 900ns (pakiety 64 bitowe)
10. Możliwość łączenia min 8 przełączników w stos
11. Tablica MAC adresów min. 16k
12. Pamięć operacyjna: min. 1GB pamięci DRAM
13. Pamięć flash: min. 4GB pamięci Flash
14. Pojemność bufora pakietów min. 2MB
15. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
16. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
17. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
18. Obsługa Q-in-Q IEEE 802.1ad
19. Obsługa Quality of Service
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
20. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
21. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
22. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
23. Wbudowany DHCP serwer i klient
24. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
25. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
26. Możliwość monitorowania zajętości CPU
27. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)

28. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
29. Wbudowany dodatkowy port Gigabit/ Ethernet do zarządzania poza pasmem - out of band management.
30. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

Obsługa Routingu IPv4

31. Sprzętowa obsługa routingu IPv4 – forwarding
32. Pojemność tabeli routingu min. 480 wpisów
33. Routing statyczny
34. Obsługa routingu dynamicznego IPv4
    a. RIPv1/v2
    b. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
35. Policy Based Routing dla IPv4
36. Obsługa DHCP/BootP Relay dla IPv4

Obsługa Routingu IPv6

37. Sprzętowa obsługa routingu IPv6 – forwarding
38. Pojemność tabeli routingu min. 240 wpisów
39. Routing statyczny
40. Obsługa routingu dynamicznego dla IPv6
    a. RIPng
    b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
41. Obsługa MLDv1 (Multicast Listener Discovery version 1)
42. Obsługa MLDv2 (Multicast Listener Discovery version 2)
43. Policy Based Routing dla IPv6
44. Obsługa DHCP/BootP Relay dla IPv6
45. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

Obsługa Multicastów

46. Statyczne przyłączenie do grupy multicast
47. Filtrowanie IGMP
48. Obsługa Multicast VLAN Registration - MVR
49. Obsługa IGMP v1 (RFC 1112)
50. Obsługa IGMP v2 (RFC 2236)
51. Obsługa IGMP v3 (RFC 3376)
52. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo

53. Obsługa Network Login
    a. IEEE 802.1x

   b. Web-based Network Login
   c. MAC based Network Login
54. Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants)
55. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
56. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
57. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
58. Obsługa Guest VLAN dla IEEE 802.1x
59. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
60. Wbudowana obrona procesora urządzenia przed atakami DoS
61. Obsługa TACACS+ (RFC 1492)
62. Obsługa RADIUS Authentication (RFC 2865)
63. Obsługa RADIUS Accounting (RFC 2866)
64. RADIUS and TACACS+ per-command Authentication
65. Bezpieczeństwo MAC adresów
   a. ograniczenie liczby MAC adresów na porcie
   b. zatrzaśnięcie MAC adresu na porcie
   c. możliwość wpisania statycznych MAC adresów na port/vlan
66. Możliwość wyłączenia MAC learning
67. Obsługa SNMPv1/v2/v3
68. Klient SSH2
69. Zabezpieczenie przełącznika przed atakami DoS
   a. Networks Ingress Filtering RFC 2267
   b. SYN Attack Protection
   c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
70. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
71. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
72. Obsługa bezpiecznego transferu plików SCP/SFTP
73. Obsługa DHCP Option 82
74. Obsługa Gratuitous ARP Protection
75. Obsługa Trusted DHCP Server
76. Obsługa DHCP Snooping
77. Obsługa DHCP Secured ARP/ARP Validation
78. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s

Bezpieczeństwo sieciowe

79. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
80. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
81. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
82. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
83. Obsługa PVST+
84. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
85. Obsługa G.8032

86. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
87. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

88. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
89. Obsługa synchronizacji czasu NTP
90. Zarządzanie przez SNMP v1/v2/v3
91. Zarządzanie przez przeglądarkę WWW – protokół http i https
92. Telnet Serwer/Klient dla IPv4 / IPv6
93. SSH2 Serwer/Klient dla IPv4 / IPv6
94. Ping dla IPv4 / IPv6
95. Traceroute dla IPv4 / IPv6
96. Obsługa SYSLOG z możliwością definiowania wielu serwerów
97. Sprzętowa obsługa sFlow
98. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
99. Obsługa RMON2 (RFC 2021)

Inne

100. Wsparcie dla technologii Data Center Bridging (802.1Qaz & 802.1Qbb)
    - DCBx Data Center Bridging Exchange Protocol
    - Priority Flow Control (PFC)
    - Enhanced Transmission Selection (ETS)
101. Obsługa skryptów CLI
102. Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
103. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym

Gwarancja

104. Urządzenie musi być objęte dożywotnią gwarancją producenta obejmującą:
    a. bezpłatne aktualizacje oprogramowania firmware,
    b. wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego od zgłoszenia awarii,
    c. wsparcia technicznego producenta poprzez infolinię, pocztę e-mail oraz telefon.
    d. W przypadku braku dożywotniej gwarancji wraz z urządzeniem należy dostarczyć kontrakt serwisowy na okres min. 5 lat.
    e. W przypadku gdy którekolwiek z wymienionych w specyfikacji funkcjonalności ograniczone są licencją czasową, należy dostarczyć taką licencję na okres min. 5 lat.

Przełączniki sieciowe dostępowy (2sztuki)

Min. 48 x 1000Base-T IEEE 802.3ab/802.3at
Obsługa IEEE 802.3x Flow Control (Full-Duplex) oraz Back Pressure (Half-Duplex), Auto MDI/MDI-X na wszystkich portach
Możliwość konfiguracji prędkości i dupleksu oraz wyłączenia FlowControl dla każdego portu
Min 4 x SFP+ IEEE 802.3ae/802.3ae - porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z
Aktywne monitorowanie przyłączonych urządzeń PoE z możliwością ponownego uruchomienia podłączonych urządzeń przez wyłączenie i włączenie zasilania
Konsola szeregowa RS-232
Łączenie urządzeń w stosy o wielkości co najmniej 6 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. Praca w topologii pierścienia.
Przepustowość magistrali stosu co najmniej 40 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie
Zasilanie AC 230V. Możliwość użycia dodatkowego zasilacza nadmiarowego
Budżet mocy dla urządzeń PoE co najmniej 370 watów. Możliwość korzystania z zasilacza podstawowego oraz nadmiarowego w celu zwiększenia budżetu mocy PoE do co najmniej 740 watów.
Pojemność przełączania nie mniej, niż 176 Gb/s. Wydajność przełączania nie mniej niż 130 Mp/s.
Architektura nieblokującą (wire-speed).
Pojemność tablicy MAC nie mniej, niż 16K. Możliwość wprowadzenia co najmniej 510 wpisów statycznych
Ilość RAM nie mniej, niż 256 MB. Pamięć Flash nie mniej, niż 32 MB
Obsługa ramek Jumbo o rozmiarze co najmniej 9210 B
Bufor pakietów nie mniej, niż 3 MB
Temperatura pracy w zakresie co najmniej od -5ºC do 50ºC.
MTBF > 300000 godzin.

Funkcjonalności warstwy 2
IGMP Snooping v3 - obsługa nie mniej, niż 500 grup multicast, w tym co najmniej 256 grup statycznych
MLD Snooping v2 - obsługa nie mniej, niż 31 grup multicast, w tym co najmniej 31 grup statycznych
IEEE 802.1D, 802.1w, 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN
Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP
Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie.
Obsługa LACP
LLDP (802.1AB) oraz LLDP-MED.
ERPS (ITU-T G.8032) w wersji co najmniej 1. Jednoczesna obsługa co najmniej 1 pierścieni
DHCP Relay (opcje 60 i 61), opcja 82, DHCP Local Relay (opcja 82). DHCP Relay dla IPv6
Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu

Obsługa sieci VLAN
802.1Q VLAN (nie mniej, niż 4094), 802.1v, GVRP
Surveillance VLAN

MAC-based VLAN
Asymmetric VLAN

Funkcjonalności warstwy 3
Wiele interfejsów IPv4 (co najmniej 16 instancji)
UDP helper
DHCP Server (co najmniej 10 pul adresowych), DHCPv6 Server (co najmniej 16 pul adresowych)
Tablica ARP co najmiej 0,5K (co najmniej 256 wpisów statycznych)
Pojemność tablicy przekazywania co najmniej 512 tras IPv4 oraz 256 takich tras dla IPv6
Pojemność tablicy routowania co najmniej 64 tras IPv4 oraz 32 takich tras dla IPv6.
Routing statyczny IPv4 (co najmniej 64 tras) oraz IPv6 (co najmniej 32 tras)
IPv6 ND

Quality of Service
QoS - co najmniej 8 kolejek. Klasyfikacja w oparciu o: port fizyczny, VLAN, MAC, EtherType, IP, DSCP, protokół, port TCP/UDP, klasa IPv6, etykieta IPv6
Mapowanie DSCP do COS
Obsługa algorytmu Strict, WRR, WDRR
Obsługa trTCM/srTCM
Limitowanie pasma TX per port (nie więcej niż co 64 kb/s)
Limitowanie pasma RX per port (nie więcej niż co 64 kb/s)

Filtrowanie ruchu
ACL w oparciu o: port przełącznika, MAC, VLAN, 802.1p, IP, DSCP, typ protokołu, port TCP/UDP, klasę IPv6, etykietę IPv6, uruchamianie reguł ACL wg kalendarza, definiowanie reguł VLAN ACL

Funkcje bezpieczeństwa
Port Security (co najmniej 120 adresów MAC per port). Funkcja Port Security Shutdown
Uwierzytelnianie 802.1X z obsługą Guest VLAN
Możliwość jednoczesnego uwierzytelniania wielu użytkowników 802.1X na porcie
Przypisywanie parametrów autoryzacyjnych z serwera RADIUS: VLAN, 802.1p, przepustowość portu, reguły ACL
Obsługa CoA
Uwierzytelnianie poprzez stronę Web
Uwierzytelnianie po MAC
Uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.
Filtrowanie w oparciu o pary IP-MAC (co najmniej 250 powiązań IP-MAC na urządzenie), DHCP Snooping, Dynamic ARP Inspection (również IPv6)
Separacja klientów przyłączonych do różnych portów
Blokowanie serwerów DHCP
MAC Blackholing
ARP Spoofing Prevention
BPDU Attack Protection
DoS Attack Protection

Unicast Storm Control (krok co najwyżej 64Kbps i 2pps), Multicast Storm Control (krok co najwyżej 64Kbps i 2pps), Broadcast Storm Control (krok co najwyżej 64Kbps i 2pps), Storm Control Port Shutdown, Storm Control Port Recovery

Zarządzanie
Uwierzytelnianie dostępu administracyjnego protokołem RADIUS i TACACS+.
Zarządzanie stosem poprzez pojedynczy adres IP
Zdalne wykrywanie urządzenia przez dedykowaną aplikację producenta przełącznika i co najmniej zmiana adresu IP urządzenia
WebGUI (obsługa IPv6), Telnet (co najmniej 4 sesji jednoczesnych) (obsługa IPv6), SSH (obsługa IPv6), konsola szeregowa (możliwość wprowadzania poleceń, możliwość konfiguracji wszystkich funkcjonalności urządzenia)
Wsparcie szyfrowania HTTP
Możliwość wykrywania urządzeń zgodnych z protokołem ONVIF, wyświetlanie informacji o rzeczywistym stanie tych urządzeń
SNMPv2, v3 (obsługa IPv6)
RMON, sFlow
Obsługa DDM
Klient DHCP oraz provisioning z zewnętrznego serwera TFTP
Klient DNS
Klient SNTP (obsługa IPv6)
Zapis logów na serwer Syslog (obsługa IPv6)
Zapis i pobieranie konfiguracji z serwera TFTP
Traceroute
Diagnostyka okablowania (co najmniej pomiar długości oraz ciągłość połączenia).
Możliwość wprowadzania opisów portów.
Wysyłanie powiadomień SNMP po pojawieniu się nowego adresu MAC w sieci.
Możliwość logowania wydawanych poleceń.
Możliwość przechowywania wielu wersji firmware.
Wsparcie 802.3az (Energy Efficient Ethernet).
Zmniejszanie pobieranej mocy poprzez wykrywanie aktywności linku na portach, administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.

Pozostałe
Dostępność bezpłatnych aktualizacji oprogramowania przez cały czas życia produktu.
Gwarancja przez cały czas produkcji urządzenia oraz przez co najmniej 5 lat po jej zakończeniu.

Macierz dyskowa (1sztuka)

Lp.	Nazwa parametru	Minimalna wartość parametru
1	Obudowa	System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''.

2	Nośniki	System musi zostać dostarczony w konfiguracji zawierającej minimum 12 dysków 4TB NL-SAS i zajmować maksymalnie 2U w szafie rack System musi ponadto wspierać dyski: - SSD: od 800GB - SAS 10k od 900GB - NL-SAS od 4TB System musi mieć możliwość rozbudowy do minimum 180 dysków oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami). Zamawiający dopuszcza rozwiązanie, które nie pozwala na taką rozbudowę w przypadku, gdy zostanie zaoferowany najwyższy z modeli macierzy skalowalny min do 500 dysków oraz pamięcią cache min 512GB. Macierz musi pozwalać i być przystosowana na rozbudowę do modelu NVME bez potrzeby wymiany dysków i kopiowania danych.
3	Kontroler	Przynajmniej dwa kontrolery wyposażone w przynajmniej 8GB cache każdy. W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.
4	Interfejsy	Oferowana macierz musi posiadać minimum - 4 porty 16Gb FC bez wkładek SFP+ - 4 porty SAS 12 Gb/s do podłączenia półek dyskowych Możliwość rozbudowy lub wymiany do co najmniej 12 portów 10GbE lub/i 8 portów 32Gb lub/i 8 portów 12Gb SS 10k
5	RAID	Wsparcie dla RAID: 0, 1, 5, 6, 10 Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 180 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych. Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy.
6	Obsługiwane protokoły	FC, iSCSI, SAS, S3, CIFS, NFS Zamawiający dopuszcza zrealizowanie protokołu CIFS, NFS i S3 za pomocą zewnętrznego oprogramowania typu Software Defined Storage.
7	Inne wymagania	Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów: Microsoft® Windows Server, Red Hat Enterprise Linux, Novell SUSE Linux Enterprise Server, VMware® ESX®, Oracle® Solaris, HP HP-UX, IBM AIX, Macierz musi posiadać funkcjonalność wykonywania snapshotów - minimum 128 per wolumen. Macierz musi posiadać funkcjonalność klonowania danych

		Macierz musi posiadać funkcjonalność replikacji danych po FC (po zainstalowaniu portów FC na macierzy) w trybie synchronicznym i asynchronicznym, oraz po Ethernecie w trybie asynchronicznym system musi pozwalać na wykonanie co najmniej do 32 jednoczesnych replikacji. Wsparcie producenta dla replikacji z istniejącą macierzą Zamawiającego. Macierz musi posiadać możliwość tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowa (ang. ThinProvisioning). Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do co najmniej 128 partycji. Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika. Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID. Z poziomu graficznego interfejsu do zarządzania musi istnieć możliwość sprawdzenia stanu zużycia dysków SSD. Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście: - wydajności i opóźnień na wolumenach - wydajności I/Ops, MB/s Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji. Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z: - Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter - VMware VASA - Microsoft Virtual Disk Service (VDS) - Microsoft Virtual Shadow Service (VSS) - Oracle Enterprise Manager – monitoring zasobów macierzowych Zamawiający dopuszcza zaoferowania zewnętrznego oprogramowania do zapewnienia integracji i monitoring w/w aplikacji np. w formie Software Defined storage. Macierz musi pozwalać na szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.

8	Gwarancja i serwis	3 lata serwisu producenta zapewniającego dostawę podzespołu zapasowego na następny dzień roboczy od diagnozy problemu. Możliwość zgłaszania awarii poprzez linię telefoniczną lub inne systemy firmy serwisującej. Dostarczony system musi posiadać również 3 lata serwisu (aktualizacje i wsparcie) producenta dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. Zepsute dyski zostają u zamawiającego

Serwerowy system operacyjny (SSO)

Należy dostarczyć serwerowy system operacyjny (SSO) spełniający poniższe wymagania dla dwóch serwerów wyposażonych w dwa procesory 8 rdzeniowe każdy: (licencja dożywotnia nie może być ograniczona czasowo)
Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie min. dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze, była w pełni kompatybilna z posiadanymi przez zamawiającego pozostałymi systemami.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1) Możliwość wykorzystania min 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania min. 64 procesorów wirtualnych oraz min 1TB pamięci RAM i dysku o pojemności co najmniej do 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z co najmniej 64 węzłów, z możliwością uruchamiania min 7000 maszyn wirtualnych.
4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18) Mechanizmy logowania w oparciu o:
    a) Login i hasło,
    b) Karty z certyfikatami (smartcard),
    c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows

c) Zdalna dystrybucja oprogramowania na stacje robocze.
d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   i. Dystrybucję certyfikatów poprzez http
   ii. Konsolidację CA dla wielu lasów domeny,
   iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f) Szyfrowanie plików i folderów.
g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i) Serwis udostępniania stron WWW.
j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
k) Wsparcie dla algorytmów Suite B (RFC 4869),
l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie conajmniej do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
   i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   iii. Obsługi min 4-KB sektorów dysków
   iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Rozbudowa posiadanych serwerów

Wykonawca dostarczy i zainstaluje w posiadanych serwerach następujące elementy:

1. Serwer DELL R530 (2sztuki):
   a) 32 GB pamięci RAM w każdym
2. Serwer DELL T440
   a) 64 GB pamięci RAM
   b) Karta sieciowa PCIe 2x porty 10GB SFP+ wraz z modułami SFP+ SR Optic 10GbE 850nm

Dostarczone komponenty muszą być certyfikowane przez producenta posiadanych serwerów.

Media konwerter (5sztuk)

Zastosowanie	Urządzenia będą pełnić funkcję zmiany medium transmisyjnego ze światłowodu na skrętke STP/UTP
Interfejs optyczny	Konektor SFP LC Przepustowość min 125/1250Mbps Tryb Pracy Pełny duplex Światłowód MM 50/125µm, 62.5/125µm, SM 9/125µm Dystans MM 2km, SM 15/30/50/80/120km, WDM 20/40/60/80km Długość Fali MM 1310nm, SM 1310,1550nm, WDM 1310Tx/1550Rx (type A), 1550Tx/1310Rx (type B)
Interfejs Elektryczny	Konektor RJ-45 Przepustowość min. 10Mbps, 100Mbps, 1000Mbps Tryb Pracy Half / Full duplex Kabel 10Base-T Kat.3, 4, 5, UTP, 100Base-TX Kat.5, 5e lub wyższy
Standardy	IEEE 802.3, IEEE 802.3u IEEE 802.3ab, 802.3z
Dodatkowe wyposażenie	Interfejsy optyczne muszą być obsadzone modułami SFP 1.25Gbps LX 1310nm LC DDM SMF 20km
Gwarancja	2 lata

Laptop (2 sztuki)

Typ	Komputer przenośny, nie dopuszcza się modyfikacji na drodze Producent-Zamawiający.
Ekran	Matowy, matryca TFT 15” z podświetleniem w technologii LED, rozdzielczość min. FHD 1920x1080, o jasności min. 300 nitów. Kontrast minimum 800:1.
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w mobilnych stacjach roboczych klasy x86, o wydajności liczonej w punktach

	równej lub wyższej procesorowi Intel Core i7-12800H na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/.
Pamięć operacyjna RAM	Min. 64 GB min 4800Mhz Możliwość rozbudowy do 64GB pamięci RAM, w tym min. 1 slot wolny
Parametry pamięci masowej	Min. 512 GB SSD PCIe 4.0 NVMe Dysk obsługujący sprzętowe szyfrowanie OPAL Możliwość robudowy do min 2 dysków SSD. Wsparcie RAID min. 0 i 1
Karta graficzna	Dedykowana karta graficzna z pamięcią własną min 4GB przeznaczona do zastosowań profesjonalnych, o wydajności liczonej w punktach równej lub wyższej karcie NVIDIA T600 na podstawie PerformanceTest w teście G3D Mark według wyników Avarage G3D Mark opublikowanych na https://www.videocardbenchmark.net/
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby min. 2 x 2W, Port słuchawek i mikrofonu typu COMBO, kamera video min. 720p z mechaniczną zasłoną obiektywu, min. dwa wbudowane mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).
Obudowa	Wykonana z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzujący się wzmocnioną konstrukcją, tzw. „business rugged”, według normy MIL-STD-810H.
Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej. Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym.
Bezpieczeństwo	Zintegrowany z płytą główną układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego zapisanego w TPM2.0 z certyfikacją TCG. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Kamera notebooka obsługująca funkcję Windows Hello (logowanie twarzą) Dostęp do podzespołów komputera musi być sygnalizowany przez czujnik otwarcia obudowy. Sygnalizacja konfigurowana z poziomu BIOS. Zamawiający uzna za równoważne dostarczenie linki zabezpieczającej typu Kensington zamykanej w taki sposób, że nie będzie możliwe otwarcie obudowy notebooka, gdy linka zabezpieczająca zostanie umieszczona i zamknięta z wykorzystaniem kluczyka w dedykowanym slocie Kensington. Komputery wyposażone w złącze

	Noble Lock muszą zostać zaoferowane z adapterem ze złącza Noble Lock komputera do Kensington.
System diagnostyczny	Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System umożliwiający wykonanie minimum następujących czynności diagnostycznych: - wykonanie testu: pamięci ram, procesora, pamięci masowej, matrycy lcd, magistrali pci-e, płyty głównej (chipset, usb), klawiatury, myszy, akumulatora (weryfikacja temperatury, liczby cykli, poziomu naładowania oraz pojemności akumulatora), ekranu dotykowego (w przypadku dotykowej matrycy) - identyfikację jednostki i jej komponentów w następującym zakresie: notebook (producent, numer konfiguracji, model, numer seryjny), bios (wersja oraz data wydania bios), procesor (nazwa, taktowanie, obsługiwane instrukcje, ilości pamięci L1, L2, L3, liczba rdzeni oraz liczba obsługiwanych wątków przez procesor), pamięć ram (ilość zainstalowanej pamięci ram, producent oraz numer seryjny poszczególnych kości pamięci wraz z obsadzeniem, taktowanie pamięci), dysk twardy (model, numer seryjny, wersja oprogramowania sprzętowego, pojemność, temperatura), LCD (producent, model, rozdzielczość), akumulator (producent, pojemność, data produkcji, liczba cykli) - możliwość zapisania wyniku przeprowadzonych testów na nośniku zewnętrznym np. USB Ponadto zaimplementowany dźwiękowy system diagnostyczny producenta umożliwiający identyfikację następujących zdarzeń: • Awaria głównej magistrali systemowej • Awaria wentylatora • Awaria modułu pamięci • Awaria karty rozszerzeń (M.2, PCIe) • Awaria modułu TPM • Awaria dedykowanej karty graficznej (PCIe) • Awaria zintegrowanej karty graficznej (w CPU) • Awaria połączenia pomiędzy jednostką, a wyświetlaczem
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS

	- daty produkcji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM oraz możliwość odczytania informacji o obłożeniu, szybkości i rodzaju z poziomu BIOS lub w zaimplementowanym systemie diagnostycznym - typie procesora i jego prędkości - MAC adresu zintegrowanej karty sieciowej - nr inwentarzowym (tzw. Asset Tag) - wymagane wolne pole do edycji przez administratora - nr seryjnym płyty głównej komputera - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość Wyłączania/Włączania technologii antykradzieżowej - Możliwość dwustopniowej preautentykacji użytkownika w BIOS z wykorzystaniem czytnika linii papilarnych - Możliwość zaawansowanego zarządzania dostępem do BIOS poprzez mechanizm wielopozowych haseł umożliwiających co najmniej: o Możliwość ustawienia hasła Administratora o Możliwość ustawienia hasła na zainstalowanym dysku SSD/HDD o Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password o Możliwość przeglądania ustawień BIOS z poziomu użytkownika bez możliwości zmiany ustawień BIOS o Możliwość zabezpieczenia hasłem aktualizacji BIOS o Możliwość adaptacji poziomu uprawnień w BIOS dla użytkownika - Możliwość ustawienia minimalnych wymagań dotyczących długości hasła POWER-On oraz hasła dysku twardego. - Obsługa haseł o długości min. 128 znaków zawierających: duże litery, małe litery, znaki specjalne, cyfry - Możliwość wymuszenia silnych haseł ustawianych w BIOS tzn. składających się z co najmniej ośmiu znaków z min. jedną małą literą, jedną dużą literą oraz jedną cyfrą. - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS - Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Autoryzacja dostępu do aktualizacji BIOS dla użytkownika, Administratora lub z poziomu Windows - Możliwość Wyłączania/Włączania zabezpieczenia przed wgraniem starszej wersji BIOS niż aktualna - Mechanizm samokontroli i samoczynnej autonaprawy, działający automatycznie przy każdym uruchomieniu komputera, który sprawdza integralność i autentyczność uruchamianego podsystemu BIOS - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, Thunderbolt 4, zintegrowanej kamery,

	modemu LTE, portów USB, bluetooth, czytnik kart pamięci, czytnik karta inteligentnych, zintegrowanej karty dźwiękowej, mikrofon, dotyku w przypadku matrycy dotykowej. - Możliwość włączenia/wyłączenia funkcji klonowania adresu MAC dla stacji dokującej - Możliwość niezależnego włączenia/wyłączenia płytki dotykowej oraz manipulatora (joysticka) - Funkcja bezpiecznego usuwania danych z dysku dostępna z poziomu BIOS
Interfejsy / Komunikacja	min, 2xUSB 3.2 Gen. 1, min. 1xThunderbolt 4, złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. wersja 2.0, RJ-45, czytnik kart SD lub microSD, czytnik smart card reader (kart inteligentnych). Złącze umożliwiające podpięcie linki antykradzieżowej. Komputer w ramach posiadanych portów musi umożliwiać dokowanie za pośrednictwem portu Thunderbolt 4 lub dedykowanego złącza umożliwiającego podłączenie mechanicznej stacji dokującej.
Karta sieciowa LAN	Min. 100/1000 wspierająca Wake on Lan, PXE Boot, HTTPs
Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX Bluetooth 5.2
Klawiatura	Klawiatura odporna na zalanie cieczą (funkcjonalność potwierdzona w ulotce katalogowej produktu), układ US, z wbudowanym joystikiem do obsługi wskaźnika myszy, klawiatura wyposażona w co najmniej 2 stopniowe podświetlanie przycisków. Klawiatura wyposażona w wydzielony blok numeryczny.
Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych – wspierający dwupoziomową preautentykację w BIOS.
Akumulator	Komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka do 80% w ciągu 60 minut. Akumulator o pojemności min. 68Wh
Certyfikaty, oświadczenia i standardy	- Dla producenta sprzętu należy dostarczyć certyfikat: o ISO 9001 o ISO 14001 o ISO 50001 □ EPEAT: Gold □ ENERGY STAR 8.0 - 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 - Oświadczenie producenta, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym - Oświadczenie producenta lub dokument pochodzący od producenta potwierdzający, że komputer spełnia standardy MIL-STD-810H.
Waga/Wymiary	Waga urządzenia z akumulatorem max. 2.3 kg Grubość notebooka nie większa niż: 23 mm

System operacyjny	Microsoft Windows 10 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.

	19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard),

	c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Gwarancja	-Minimum 36 miesięcy gwarancji producenta sprzętu, świadczonej w miejscu użytkowania (on-site). -Wsparcie techniczne producenta komputera– dostępne w trakcie obowiązywania gwarancji na urządzenie obejmujące co najmniej: wsparcie dla zakupionego sprzętu jak również dostarczonego wraz ze sprzętem oprogramowania OEM, możliwość weryfikacji konfiguracji fabrycznej zakupionego sprzętu, możliwość weryfikacji statusu naprawy, - Wsparcie techniczne świadczone w dni robocze, minimum w godzinach 8-17 w języku polskim - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. -Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta oferowanego komputera (automatyczna identyfikacja komputera, konfiguracja fabryczna, Rodzaj gwarancji, data wygaśnięcia gwarancji, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

System monitoringu infrastruktury (1 sztuk)

Rozwiązanie do monitorowania zasobów IT musi umożliwiać:

1. Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat.
2. Zapewnienia równoległego dostępu do systemu dla wielu użytkowników.
3. Ograniczania użytkownikom dostępu do wybranych grup hostów.
4. Monitorowania serwerów fizycznych.
5. Monitorowania urządzeń sieciowych.

6. Monitorowania stanu połączeń VPN.
7. Monitorowanie interfejsów sieciowych przełączników, ruterów, serwerów (b/s, p/s,err/s).
8. Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.
9. Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.
10. Rozbudowę systemu o monitorowanie kolejnych urządzeń.
11. Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.
12. Grupowanie hostów.
13. Definiowanie planowanych przerw serwisowych dla hostów i usług.
14. Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).
15. Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania powiadomień; konfiguracje przerw serwisowych).
16. Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).
17. Globalne wyłączanie powiadomień.
18. Prezentację stanu urządzeń na mapie.
19. Monitorowanie transakcji dla serwisów WWW. Transakcje będą składały się z kilku kroków.
20. Powiadamianie użytkownika o problemach przez e-mail.
21. Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie.
22. Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników.
23. Prezentację danych na dashboardach.
24. Elastyczną konfigurację dashboardów, wybór elementów
25. Wizualizację stanu działania całej infrastruktury na jednym dashboardzie
26. Tworzenie indywidualnych dashboardów przez użytkowników.
27. Definiowanie różnych wartości progowych alertów na poziomie globalnym grupy urządzeń, pojedynczych urządzeń, pojedynczych usług
28. Monitorowanie serwerów za pomocą agentów
29. Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Orade Application Server.
30. Monitorowanie Active Directory.
31. Monitorowanie serwerów plików, udziałów sieciowych.
32. Monitorowanie statusu serwerów Apache.
33. Monitorowanie baz danych:
    a) ORACLE,
    b) MySQL,
    c) Postgress.
34. Monitorowanie urządzeń przez następujące protokoły:
    a) SNMP,
    b) WMI,
    c) IPMI.
35. Konfigurację oprogramowania systemu monitorowania poprzez interfejs

36. Monitorowanie poprawności działania DNS
37. Monitorowanie środowiska VMware.
38. Monitorowanie środowiska Hyper-V.
39. Monitorowanie działania serwera czasu NT P.
40. Monitorowanie offsetu czasu na serwerach.
41. Monitorowanie ping - czasy odpowiedzi, straty pakietów.
42. Monitorowanie zajętości miejsca na poszczególnych partycjach.
43. Monitorowanie obciążenia dysków.
44. Monitorowanie wykorzystania pamięci RAM.
45. Monitorowanie obciążenia systemu.
46. Monitorowanie logów systemowych Windows.
47. Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.
48. Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.
49. Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business
50. Intelligence)
51. Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe
52. Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów).
53. Wykrywanie niestabilnie działających usług.
54. Monitorowanie dostępności stron internetowych.
55. Inwentaryzację zasobów sprzętowych i oprogramowania.
56. Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).
57. Możliwość ustawienia interwału pomiarowego 1 sekunda.
58. Wykonawca dokona instalacji i konfiguracji systemu. Do systemu należy podłączyć minimum hosty wirtualizacyjne wraz z maszynami wirtualnymi, przełączniki sieciowe, urządzania UTM, macierze dyskowe.
59. System musi być uruchomiony w postaci maszyny wirtualnej na posiadanym przez Zmawiającego środowisku.

Wraz z systemem należy dostarczyć, zamontować oraz skonfigurować 2 sztuki monitorów spełniających poniższe minimalne wymagania:

Przekątna ekranu	Min. 48 cali
Typ matryce	LED, matowa
Proporcje ekranu	16:9
Rozdzielczość	Min. 3840x2160 (4K UHD)
Rozstaw pikseli (mm)	Maks. 0.285 x 0.285
Jasność	Min. 500 nit
Współczynnik kontrastu	Min. 4000:1
Kąt widzenia (poziom/pion)	Min. 178/178
Czas reakcji matrycy (G-do-G)	Maks. 8ms
Czas pracy zalecany przez producenta	24 godz./dzień (praca ciągła)
Złącza	Min 1xHDMI, min. 1xDP, mim 1xRJ-45
Mocowanie	VESA
Łączność	Wi-FI

Gwarancja	3 lata

Szkolenie dla pracowników

Wykonawca przeprowadzi szkolenie dla pracowników Zamawiającego (co najmniej 150 osób). Szkolenie będzie przeprowadzone w 3 turach po min. 2 godzinny zegarowe. Zamawiający zapewni salę szkoleniową oraz rzutnik.

Zakres szkolenia - podstawy cyberbezpieczeństwa (2 godziny zegarowe):

- Podstawy prawne i wymagania w zakresie bezpieczeństwa informacji.
- Międzynarodowe normy bezpieczeństwa.
- Bezpieczeństwo organizacyjne.
- Aspekty ciągłości działania w bezpieczeństwie informacji.
- Podstawy ataków socjotechnicznych.
- Jak bronić się przed atakami socjotechnicznymi?
- Bezpieczeństwo w cyberprzestrzeni.
- Praktyczne zabezpieczanie danych na komputerze.
- Szyfrowanie przechowywanych i przesyłanych danych osobowych.
- Zabezpieczanie danych w formie papierowej.
- Dyskusja.

Szkolenie dla administratorów

Wdrożenie

Konfiguracja połączeń sieciowy

a) W ramach projektu „Budowa Światłowodu dla Miasta Darłowo” Zamawiający wybudował połączenia światłowodowe pomiędzy jednostkami podległymi a UM Darłowo. Wykorzystany został światłowód jednodomowy 30J rozchodzący się po 4 włókna na jednostkę (dla MOPS 6 włókien).
b) W ramach zadania wykonawca podłączy urządzenie aktywne i skonfiguruje połączenia sieciowe. Funkcje centralnego routera będzie pełnił zaoferowany system firewall.
c) Konfiguracja połączeń musi umożliwiać udostępnienie połączenia do Internetu oraz e-usług świadczonych z UM Darłowo.
d) Lista jednostek podległych (szczegółowy wykaz prac i konfiguracji zostanie udostępniona na wizji lokalnej):
    i. Miejski Ośrodek pomocy Społecznej w Darłowie
    ii. Miejski Zarząd Budynków Komunalnych w Darłowie
    iii. Straż Miejska w Darłowie
    iv. Przedszkole nr 2 im. Janiny Porażińskiej w Darłowie
    v. Dawny dworzec PKP w Darłowie
    vi. DOK, MPGK, Wyspa Łososiowa

e) Montaż urządzeń szafie rack
f) Nadanie adresu IP
g) Konfiguracja dostępu SSH
h) Zmiana haseł dostępu
i) Utworzenie klastra firewalli.
j) Aktualizacja oprogramowania do najnowszej możliwej wersji na urządzeniach UTM Darłowo
k) Stworzenie do 500 reguł bezpieczeństwa
l) Konfiguracja tuneli VPN (Site-to-Site i Client-to-Site), po stronie wykonawcy będzie instalacja odpowiednich klientów VPN na komputerach użytkowników – około 50 komputerów
m) Konfiguracja routingu
n) Utworzenie polityk bezpieczeństwa
o) Wdrożenie funkcjonalności DPI
p) Wdrożenie deszyfracji protkokołu SSL
q) Stworzenie klastra wysokiej dostępności
r) Przepisanie konfiguracji VLAN z obecnego rozwiązania Zamawiającego do nowego klastra UTM
s) Konfiguracja firewall, reguły przychodzące i wychodzące na podstawie obecnie działających usług
t) Konfiguracja ochrony przed malware, exploitami oraz stronami zawierającymi złośliwy kod
u) Uruchomienie i konfiguracja systemu do zbierania logów z systemu firewall
v) Wdrożenie PKI oraz konfiguracja polityki za pomocą których przeprowadzona zostanie dystrybucja certyfikatów.
w) Rekonfiguracja wykorzystywanych przeglądarek www przez zamawiającego do pracy z włączoną deszyfracją protokołu SSL na firewall.
x) Konfiguracja routingu dynamicznego OSPF na urządzeniach UTM w UM Darłowo.
y) Migracja routingu wraz z całą konfiguracją sieci, do nowo utworzonego w Urzędzie Miejskim klastra UTM, z lokalizacji wymienionych poniżej:
    i. Miejski Zarząd Budynków Komunalnych w Darłowie
    ii. Straż Miejska w Darłowie
    iii. Przedszkole nr 2 im. Janiny Porażińskiej w Darłowie
    iv. Dawny dworzec PKP w Darłowie
z) Utworzenie stref bezpieczeństwa dla każdej lokalizacji ujętej w projekcie.
aa) Wdrożenie routingu OSPF po stronie UM Darłowo, Miejski Ośrodek pomocy Społecznej w Darłowie w celu optymalnej wymiany danych pomiędzy jednostkami.
bb) Utworzyć połączenie L2 pomiędzy Miejskim Ośrodku pomocy Społecznej, a UM Darłowo.
cc) Transfer wiedzy do klienta na temat obsługi zaproponowanej konfiguracji

Relokacja urządzeń

a) Wykonawca przeniesie urządzenia znajdujące się w szafie 27U w UM Darłowo do nowej szafy 42U posiadanej przez Zamawiającego. Sprzęt znajdujący się w szafie wymagający relokacji: krosownica światłowodowa, panel termostatu wentylacji, switch eth oraz switch światłowodowy, 3x patchpanele, serwer wraz macierzą dysków, QNAP, UPS, rejestrator oraz drobne podzespoły typu: media konwertery, bramki VoIP, transmiter HDMI.
b) Pustą szafę rack 27U należy przetransportować do MOPS w Darłowie w której zostaną zainstalowane dostarczone przez Wykonawcę urządzenia w ramach zamówienia.

c) Wykonawca wykona niezbędne połączenia światłowodowe oraz miedziane pomiędzy szafami rack w MOPS Darłowo ewentualnie relokacje niezbędnych urządzeń między szafami.
d) Wykonawca przeprowadzi relokację w taki sposób, aby zapewnić ciągłość działania systemów Zamawiającego. Zamawiający dopuszcza przerwę w działaniu systemów nie dłuższą niż 2 godziny w godzinach pracy Urzędu Miejskiego. Pozostałe prace nie zakłócające ich działanie mogą być wykonywane w trakcie godzin pracy Urzędu. Zasada dotyczy zarówno Urzędu Miejskiego w Darłowie jak i MOPS. Planowane przerwy w działaniu systemów Zamawiającego należy uzgodnić z Zamawiającym.

Macierz dyskowa i serwer

a) Podłączenie macierzy dyskowej z wykorzystaniem światłowodu w celu zapewnienia replikacji danych pomiędzy główną serwerownią a zapasową
b) Wykonawca zainstaluje i skonfiguruje nowe przełączniki ISCSI w UM Darłowo, a posiadany przełącznik przeniesie do zapasowej serwerowni w celu podłączenia dostarczonej macierzy dyskowej oraz posiadanego serwera.
c) Wykonawca zmodernizuje również serwery w UM Darłowo i MOPS o komponenty opisane w „Rozbudowa posiadanych serwerów”

Testy powdrożeniowe

Po dokonaniu całości wdrożenia należy:
a) przeprowadzić testy poprawności działania całej infrastruktury
b) przygotować dokumentację powykonawczą zawierająca listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów, schematem połączeń logicznych i fizycznych wraz z adresacjami i mapą sieci (reguły firewall)
c) Ze względu na krytyczne aplikacje które będą dostępne z sieci publicznej, Wykonawca przeprowadzi testy podatności systemów (testy penetracyjne). Testy będą polegały na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

- urządzenia dedykowane (embeded), na przykład routery i przełączniki;
- punkty styku z sieciami obcymi
- zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz
- Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na:
  - określenie błędów w konfiguracji skutkujących powstaniem podatności na atak;
  - wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk;
  - Badaniu będą podlegały następujące systemy:
    - ✓ rodzina Microsoft Windows Server (do poziomu weryfikacji poprawek Windows Update włącznie);
    - ✓ Linux 2.4.x, 2.6.x, 3.x.x;
    - ✓ IBM AIX;
    - ✓ CISCO IOS;
    - ✓ Microsoft SQL;
    - ✓ MySQL;

Badanie zostanie zakończone raportem. Forma i zakres raportu musi być zaakceptowany przez dział informatyki Zamawiającego przed zakończeniem projektu.

Szkolenie i prezentacja wdrożonych rozwiązań

Po wykonaniu testów powdrożeniowych zakończonych akceptowalnymi wynikami, w uzgodnionym z Zamawiającym terminie jednak nie później niż 14 dni od zakończenia prac, Wykonawca dokona prezentacji i przeszkolenia w zakresie: obsługi dostarczonych rozwiązań i urządzeń tj.: sterowania, analizy ruchu sieciowego oraz pracy urządzeń, przeglądów i konserwacji firmware oraz hardware. Przekaże pozostałą wiedzę niezbędną do prawidłowej i bezpiecznej ich eksploatacji. Przedstawi i omówi optymalny sposób zbierania, interpretacji oraz rekomendowane postępowania na wypadek wystąpienia alarmów i ostrzeżeń, jakie mogą się pojawić podczas ich użytkowania. Zapewni telefoniczne i e-mailowe bezpłatne roczne wsparcie merytoryczne (asystę) w tym zakresie i pomoc w organizacji naprawach gwarancyjnych.

Wymagania wykonawcy

Ze względu na zaawansowane wdrożenie dotyczące krytycznych aplikacji Zamawiającego, wymaga się aby Wykonawca dysponował odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia tj. do wykazania, że dysponuje lub będzie dysponować co najmniej:

- minimum 2 osobami posiadającymi wiedzę i doświadczenie w zakresie implementacji środowisk sieciowych i systemowych opartych na posiadanych przez Zamawiającego platformach Microsoft Server, obejmujące instalowanie i konfigurowanie elementów systemów oraz wiedzę i doświadczenie w zakresie zarządzania tymi środowiskami i rozwiązywania dotyczących ich problemów, obejmujące administrowanie systemami i obsługę ich użytkowników przy spełnieniu wymagań dla Microsoft Certified Solutions Associate (MCSA) lub wymagań równoważnych, tj., określonych na nie niższym poziomie jakości, potwierdzone certyfikatem Microsoft Certified Solutions Associate (MCSA) lub innym równoważnym dokumentem (zaświadczeniem);
- minimum 2 osobami posiadającymi wiedzę i doświadczenie w zakresie definiowania i charakteryzowania najważniejszych technik ataków stosowanych przez hakerów oraz identyfikowania i analizowania podatności na ataki hakerów w organizacji a także w tworzeniu polityki na urządzeniach IDS/IPS dotyczącej wykrywania włamań, spełniającej wymagania dla Certified Ethical Hacker (CEH) lub inne równoważne, tj. określone na nie niższym poziomie jakości niż CEH, potwierdzone certyfikatem ukończeniem szkolenia Certified Ethical Hacker (CEH) lub innym tożsamym dokumentem (zaświadczeniem) ;
- minimum 2 osobami posiadającymi wiedzę i doświadczenie w z zakresu konfiguracji i rozwiązywania problemów na posiadanych przez Zamawiającego przełącznikach sieciowych Extreme Networks przy użyciu praktyk spełniających wymagania określone dla Extreme Certified Specialist Campus EXOS lub inne równoważne, tj. określone na nie niższym poziomie jakości niż ECS Campus EXOS , potwierdzone certyfikatem Extreme Certified Specialist Campus EXOS lub innym równoważnym dokumentem (zaświadczeniem)

- minimum 1 osobą posiadającą wiedzę i doświadczenie z zakresu konfiguracji i rozwiązywania problemów na posiadanych przez Zamawiającego firewallach Sonicwall NSA2600 przy użyciu praktyk spełniających wymagania określone dla Certified SonicWall Security Professional lub inne równoważne, tj. określone na nie niższym poziomie jakości niż Certified SonicWall Security Professional, potwierdzone certyfikatem Certified SonicWall Security Professional lub innym równoważnym dokumentem (zaświadczeniem)
- minimum 1 osobą posiadającą wiedzę i doświadczenie z zakresu konfiguracji i rozwiązywania problemów z posiadanym przez Zamawiającego oprogramowaniem do wykonywania kopii zapasowej VEEAM. Przy użyciu praktyk spełniających wymagania dla VEEAM Veeam Availability Suite v10: Configuration and Management (VMCE10-VASCM) lub inne równoważne, tj. określone na nie niższym poziomie jakości niż Veeam Availability Suite v10: Configuration and Management (VMCE10-VASCM) lub innym równoważnym dokumentem (zaświadczeniem).