**Załącznik nr 6 do SWZ**

**Szczegółowy Opis Przedmiotu Zamawiania**

**Obsługa sieci (UTM) 1 klaster ( 2sztuki ) z serwisem i licencją na 2 lata**

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie

konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.

3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.

4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge

warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).

5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów

wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.

7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.

8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie

konfigurowalnych, zestawów reguł firewall.

9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.

10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez

administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.

15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.

18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.

19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.

21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).

26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

27. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).

28. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.

29. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

30. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

31. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

32. Ochrona antyspam ma działać w oparciu o:

a. białe/czarne listy,

b. DNS RBL,

c. Skaner heurystyczny.

33. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.

34. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

35. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

36. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:

a. PPTP VPN,

b. IPSec VPN,

c. SSL VPN.

37. SSL VPN ma działać co najmniej w trybach tunelu i portalu.

38. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

39. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)

40. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

41. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.

42. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

43. Urządzenie ma posiadać wbudowany filtr URL.

44. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii

tematycznych stron internetowych.

45. Administrator ma mieć możliwość dodawania własnych kategorii URL.

46. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

a. blokowanie dostępu do adresu URL,

b. zezwolenie na dostęp do adresu URL,

c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej

przez administratora.

47. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.

48. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.

49. Filtr URL musi uwzględniać komunikację po protokole HTTPS.

50. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

51. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

52. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

53. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:

a. lokalną bazę użytkowników (wewnętrzny LDAP),

b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),

c. usługę katalogową Microsoft Active Directory.

54. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.

55. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:

a. SSL,

b. Radius,

c. Kerberos.

56. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

57. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.

58. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

59. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).

60. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).

61. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

62. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

63. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

a. równoważenie względem adresu źródłowego,

b. równoważenie względem połączenia.

64. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

65. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza

podstawowego (tzw. Failover).

66. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

67. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).

68. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

69. Urządzenie ma umożliwiać statyczne trasowanie pakietów.

70. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania

statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza

podstawowego.

71. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

72. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

73. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

74. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

75. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

76. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

77. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

78. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)

79. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

80. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.

81. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do

przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.

83. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

84. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora ( script recording ).

85. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).

86. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.

87. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

88. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

89. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

a. manualnego eksportu do pliku w dowolnym momencie czasu,

b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer

zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz

dziennie, raz w tygodniu, raz w miesiącu

90. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

91. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

92. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

93. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i

przeglądania logów zebranych na urządzeniu.

94. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

95. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.

96. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.

97. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.

98. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.

99. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i

tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.

100. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.

101. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

102. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

103. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).

104. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

105. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci

skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie

określenia bramy, serwerów DNS, nazwy domeny).

106. Urządzenie ma posiadać usługę DNS Proxy.

107. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.

108. Urządzenie musi mieć zaimplementowane Open API

109. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

110. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

111. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak

przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

GWARANCJA I SERWIS

112. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy

systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.

113. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

114. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.

115. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.

116. Liczba portów Ethernet 2,5Gbps – min. 8.

117. Liczba portów światłowodowych 1Gbps – min. 1.

118. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.

119. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.

120. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.

121. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.

122. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.

123. Maksymalna liczba tuneli VPN IPSec – minimum 100.

124. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.

125. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.

126. Obsługa interfejsów 802.11q (VLAN) – minimum 128

127. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.

128. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.

129. Urządzenie nie ma limitu na liczbę użytkowników.

130. Liczba reguł filtrowania – minimum 8 192.

131. Liczba tras statycznego routingu – minimum 512.

132. Liczba tras dynamicznego routingu – minimum 10 000.

133. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.

134. Urządzenie musi być wyposażone w moduł TPM.

**Macierz ( serwer NAS ) 1 szt**

|  |  |
| --- | --- |
| Procesor | Min. AMD Ryzen V1500B 4-core 2.2 GHz |
| Obudowa | Rack 2U o wymiarach 88 × 482 x 407,5 mm |
| Montaż RACK | Tak; do szafy RACK 19’; szyny teleskopowe w zestawie |
| Pamięć RAM | 8GB pamięci SO-DIMM DDR4 ECC (możliwość rozszerzenia do 32 GB) |
| Ilość obsługiwanych dysków | 8 dysków o maksymalnej pojemności 16TB każdy z możliwością podłączenia zewnętrznej półki, która rozszerza pojemność serwera o kolejne 4 dyski |
| Zainstalowane dyski | 8 dysków o pojemności 4TB każdy, znajdujących się na liście zgodności producenta macierzy; możliwość aktualizacji oprogramowania dysków z poziomu serwera NAS |
| Interfejsy sieciowe | 4 x Gigabit (10/100/1000); Wsparcie dla Link Agregation2 x 10GbE SFP+ - możliwość zastosowania dodatkowej karty PCIe; |
| Porty | 2 x USB 3.2, 1 x eSATA, 1x PCIe 3 x 4-liniowe gniazdo x8, port konsoli x1 |
| Wskaźniki LED | Power on, Status, HDD1 -8 |
| Obsługa RAID | Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR,RAID 1,5,6,10 |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| Licencja na Kamery IP | W zestawie dwie licencje na jedną kamerę z możliwością rozszerzenia do 40. |
| Protokoły | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) |
| Usługi | Wsparcie dla High AvailabilitySerwer VPNSerwer pocztowy dla kilku domenStacja monitoringuWindows ACLIntegracja z Windows ADSFirewall z kontrolą ruchuSerwer WWWSerwer plikówManager plików przez WWWSzyfrowana replikacja zdalna na kilka serwerów w tym samym czasieAntyvirusKlient VPNUsługa DDNSOprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware |
| Obsługa migawek | • Maksymalna liczba migawek folderów współdzielonych: 1 024• Maksymalna liczba migawek systemu: 65 536 |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów, |
| Język GUI | Polski, Angielski |
| Gwarancja i serwis | 4 lat gwarancji  |
| Waga | Max. 12 KG |
| Pobór mocy | Max. 62W / Hibernacja dysków max. 30W |
| Certyfikaty  | EAC, VCCI, CCC, RCM, KC, FCC, CE, BSMI |
| System plików | Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT\*(z dodatkową licencją) |
| Liczba wolumenów | Do 64  |
| Liczba iSCSI Targetów | Do 128 |
| Liczba iSCSI LUN | Do 256 |
| Liczba kont użytkowników | 2048 |
| Liczba grup | 256 |
| Liczba udziałów | 512 |
| Ilość jednoczesnych połączeń | 1000 dla CIFS/AFP/NFS/FTP/WebDAV; 2,000 po rozszerzeniu RAM |
| Zasilanie | Zasilacz 2x 350W |
| Chłodzenie | FAN x 2 80 x 80 mm |

**Zarządzany przełącznik wielowarstwowy (48 portów) 2 szt**

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

* Ilość portów 48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
* Chłodzenie od przodu do tyłu obudowy
* Możliwość instalacji redundantnego zasilacza
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 16Mb
* MTBF min. 578472 godzin
* Wydajność min. 130,9 Mp/s
* Przepustowość min. 176 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Ilość interfejsów IP 128
* Double VLAN Tagging (QoQ)
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
* Zasilacz z certyfikatem 80+
* CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
* Class A, EN 61000-3-3:2013, EN 55024:2010
* VCCI : VCCI-CISPR 32:2016, Class A
* RCM: AS/NZS CISPR 32:2013 Class A
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
* ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
* BSMI: CNS 13438 Class A

**Zarządzany przełącznik wielowarstwowy ( 8x8 ) 2 szt**

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

* Ilość portów 8 portów SFP+ oraz 8 portów 10GBaseT niezależne
* Chłodzenie od przedu do tyłu obudowy
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 16Mb
* MTBF min. 196120 godzin
* Wydajność min. 238 Mp/s
* Przepustowość min. 320 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Minimalna ilość przełączników w stosie: 8
* Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Ilość interfejsów IP 128
* Double VLAN Tagging (QoQ)
* Yes
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu

**UPS w obudowie rack 2 szt**

|  |  |
| --- | --- |
| Opis | Układ faz 1:1 |
| SNMP do zarządzania UPS. |
| Zasilacz do montażu w szafie RACK. |
| Baterie wewnątrz zasilacza UPS. |
| Szyny do montażu w szafie Rack. |
| Autonomia – 18 MINUT DLA 1000 W |
| Moc | **minimum** 3 kVA/ 3 kW |
| Inne | - Topologia True Online z podwójnym przetwarzaniem |
| - Wyświetlacz LCD umożliwiający dokonywania ustawień oraz kontroli stanu pracy |
| - Możliwość zasilania z generatora |
| - Funkcja odłączania zasilania |
| - Akumulatory wymieniane w czasie pracy (tzw. Hot-Swap) |
| - Funkcja „zimnego startu” |
| - Oprogramowanie komunikacji kompatybilne z systemem Windows |

**System DLP (zapobieganie niekontrolowanemu wyciekowi informacji z firmy ) 1 szt**

1. System operacyjny:

a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi

b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi

c. MacOS 12 lub nowszy.

2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.

3. Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. MS SQL Express, c. AzureSQL S3 lub nowsze.

4. Pomoc i dokumentacja programu dostępne w języku angielskim.

5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.

6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.

7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.

8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.

9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.

10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.

11. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.

12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.

13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.

14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).

15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.

16. System musi rejestrować zdarzenia aktywności stacji roboczej, takie jak logowanie, wylogowanie, włączenie, wyłączenie, blokada, odblokowanie i przejście w stan bezczynności.

17. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.

18. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.

19. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.

20. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.

21. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.

22. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.

23. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.

24. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.

25. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.

26. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.

27. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych, jak i sieciowych.

28. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.

29. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.

30. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.

31. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.

32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.

33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.

34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.

35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.

36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach

**Program antywirusowy 30 stanowisk licencja na 2 lata**

**Administracja zdalna w chmurze**

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania

antywirusowego.

2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu

interfejsu WWW.

3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.

4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na

podstawie unikatowego identyfikatora sprzętowego stacji.

5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP

Proxy.

6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.

7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas

logowania do konsoli administracyjnej.

8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników

w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem,

zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać

możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez

producenta.

10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych

komputerów.

11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego

warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki

muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan

funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie,

przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo,

comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu

agenta w grupie dynamicznej.

**Ochrona stacji roboczych**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

2. Rozwiązanie musi wspierać architekturę ARM64.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu

adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz

podłączeniem komputera do sieci botnet.

5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych,

niebezpiecznych oraz podejrzanych aplikacji.

6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych,

zapisywanych i wykonywanych plików.

7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub

pojedynczych plików "na żądanie" lub według harmonogramu.

8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych

oraz dysków sieciowych i dysków przenośnych.

9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania

wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy

kontrolnej (SHA1) oraz lokalizacji pliku.

10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i

IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta

pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta

pocztowego).

12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych

protokołów HTTPS, POP3S, IMAPS.

13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden

wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody

heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z

jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod

jednocześnie.

14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w

tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci

masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń

Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń

przenośnych.

15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup

urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń

minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

• tryb automatyczny z regułami, gdzie program automatycznie tworzy i

wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych

przez użytkownika,

• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w

przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone

przez użytkownika,

• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i

użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez

użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie

przełączyć się w tryb pracy oparty na regułach,

• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o

szczególnie podejrzanych zdarzeniach.

17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny

raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:

zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i

sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu

operacyjnego, pliku hosts, sterowników.

18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania

wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić

zagrożenie bezpieczeństwa.

19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika

detekcji.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego

korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika

poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem

systemu operacyjnego.

22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego

Microsoft Outlook.

23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala

tylko na połączenia wychodzące,

• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane

połączenie,

• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i

wychodzący, zezwalając tylko na połączenia skonfigurowane przez

administratora,

• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające

na połączenia przychodzące i wychodzące. Administrator musi posiadać

możliwość konfigurowania czasu działania trybu.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez

Użytkownika.

26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor

ramki przeglądarki oraz informację na ramce przeglądarki.

27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron

internetowych.

28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co

najmniej 140 kategorii i podkategorii.

29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania

uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych,

klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

**Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz

Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu

Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise

Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi

zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu

adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden

wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody

heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość

wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu

metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika

detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie

będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa,

skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących

się w usłudze chmurowej OneDrive.

10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście

(HIPS).

11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika

poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed

uruchomieniem systemu operacyjnego.

13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników

danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci

masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek

USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM

oraz urządzeń przenośnych.

14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i

tworzyć dla nich odpowiednie wyjątki.

15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii

w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co

najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup

za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej,

działającej z poziomu przeglądarki internetowej.

19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i

instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni

wspierać rozwiązanie Dell EMC Isilon.

21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów.

Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku

awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy

całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

**Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku

Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.

2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w

systemach macOS (FileVault).

3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie

użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także

możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w

pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i

dokładne.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy

urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do

ładowarki).

4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.

5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego

zarządzania, która umożliwi:

a. usunięcie zawartości urządzenia,

b. przywrócenie urządzenie do ustawień fabrycznych,

c. zablokowania urządzenia,

d. uruchomienie sygnału dźwiękowego,

e. lokalizację GPS.

6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych

aplikacji.

7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

a. nazwę aplikacji,

b. nazwę pakietu,

c. kategorię sklepu Google Play,

d. uprawnienia aplikacji,

e. pochodzenie aplikacji z nieznanego źródła.

**Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.

3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do

chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam,

dokumenty oraz inne pliki typu .jar, .reg, .msi.

4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki

muszą zostać usunięte z serwerów producenta.

5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru

przesyłanych próbek.

6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub

folderów z przesyłania.

7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich

wspieranych produktów.

8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane

do analizy.

9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji

roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie

chronione.

10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach

roboczych.

11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub

administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć

jakie pliki zostały wysłane do analizy oraz przez kogo.

12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może

zakończyć się z wynikiem:

a) Czysty,

b) Podejrzany,

c) Bardzo podejrzany,

d) Szkodliwy.

13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania

uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych,

klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość

wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z

której administrator może przywrócić dowolne pliki oraz utworzyć dla niej

wyłączenia.

**Moduł XDR**

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu

WWW.

2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli

administracyjnej tego samego producenta.

3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po

których nie zostanie wyzwolony alarm bezpieczeństwa.

5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.

6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do

utworzonego wykluczenia.

7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę

procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę

komputera, grupę, użytkownika.

8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu,

nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać

możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach

kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz

konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików

wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego

procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę

firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz

reputację i popularność pliku.

11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać

możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich

zablokowania.

12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na

stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.

Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub

niebezpieczny.

13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość

szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi

posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej:

modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików

wykonywalnych.

15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli

zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji

szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu

antywirusowego, administrator musi mieć możliwość podglądu informacji

dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym

przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor,

pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia

peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz

wylistowanie zainstalowanego oprogramowania firm trzecich.

16. Konsola administracyjna musi mieć możliwość tagowania obiektów.

17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z

możliwością wykonywania poleceń powershell

**Program do tworzenia i zarządzania kopiami bezpieczeństwa - 6 lic bezterminowych na stacje robocze z serwisem na dwa lata**

1. Pełne wsparcie dla systemów rodziny MicrosoftWindows Server: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Storage Server 2012 R2 Essentials, Windows Server 2008 R2 Foundation, Windows Server 2008 Foundation z SP2 lub wyższy.
2. Pełne wsparcie dla systemów rodziny Windows Small Business Server: Windows Server 2012 R2 (Essentials, Foundation), Windows Server 2012 (Essentials, Foundation), Windows Small Business Server 2011, Windows Small Business Server 2008 (Standard i Premium), Windows Server 2008 R2 Foundation.
3. Pełne wsparcie dla środowisk wirtualnych: VMware Workstation, VMware ESX/ESXi, Microsoft Hyper-V, Microsoft Virtual PC, Microsoft Virtual Server, Oracle VirtualBox, Citrix XenServer, Linux KVM, ProxMox, Red Hat Enterprise Virtualization (RHEV), Stratos everRun.
4. Wsparcie dla 32 i 64-bitowych systemów Microsoft.
5. Wsparcie systemów plików: FAT16, FAT16X, FAT32, FAT32X, NTFS.
6. Wsparcie dla dysków z tablicą partycji MBR oraz GPT
7. Pełne wsparcie dla systemów Ubuntu 14.04, 16.04, 18.04, 20.04, CentOS 7, Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Oracle Linux (wszystkie systemy 64-bitowe).
8. Wsparcie systemów plików: ext2, ext3, ext4, XFS.
9. Program i wsparcie techniczne dostępne w języku polskim
10. Wsparcie dla 32 i 64-bitowych systemów Microsoft: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
11. Backup obejmuje kopie całego systemu operacyjnego wraz z konfiguracją oraz zainstalowanymi aplikacjami i plikami.
12. Program umożliwia skonfigurowanie różnych schematów wykonywania backupu: w trybie pełnym, backupy przyrostowe lub tryb mieszany. Harmonogram przyrostowy powinien umozliwiać backup z częstotliwością min. co 15 minut.
13. Istnieje możliwość wykonywania backupów pełnych i przyrostowych na dyski lokalne, dyski sieciowe, SAN, NAS, dyski USB, Firewire.
14. Program wykonuje kopie zapasowe (backupy) na poziomie sektorów czyli backup przyrostowy zawiera tylko zmienione sektory na dysku a nie np. całe pliki.
15. Program nie wymaga oddzielnego serwera zarządzającego backupem, a harmonogram zadań tworzenia backupów dla danej maszyny jest przechowywany bezpośrednio na tej maszynie.
16. Możliwe jest tworzenie kopii zapasowej w automatycznym trybie hot backupu (bez korzystania ze skryptów zamykających i uruchamiających bazy czy programy). Hot backup powinien pozwalać na backup systemu, aplikacji i baz danych takich MS SQL, MS Exchange, Active Directory, Share Point, Oracle od wersji 11g.
17. Do wykonywania kopii zapasowej wykorzystywana jest technologia Microsoft VSS oraz certyfikowany sterownik Microsoftu.
18. Program umożliwia wykonywanie kopii zapasowej dysku bez konieczności uruchamiania systemu operacyjnego za pomocą bootowalnej płyty lub pendrive’a z systemem i oprogramowaniem dostarczanym przez producenta rozwiązania backupowego.
19. Rozwiązanie pozwala na okresową weryfikacje, konsolidację oraz retencję łańcucha backupu przyrostowego z możliwością konfiguracji po jakim czasie mają się one wykonać.
20. Rozwiązanie musi umożliwiać tworzenie backupu przez łącze 3G i WiFi.
21. Podczas tworzenia kopii zapasowej program generuje plik sumy kontrolnej (md5) dla pliku backupu w celu kontroli plików backupu.
22. Program posiada narzędzie pozwalające na automatyczną weryfikację tworzonych plików backupu za pomocą okresowego uruchamiania backupowanego systemu operacyjnego w maszynie wirtualnej, oraz wysłanie zrzutu ekranu z tak uruchomionego systemu do administratora za pomocą wiadomości email.
23. Program umożliwia konwersje kopii zapasowej do plików dysków maszyn wirtualnych w formacie VHD, VMDK, VHDX.
24. Program umożliwia replikację wykonanych plików kopii zapasowych na dyski lokalnie, dyski sieciowe lub do lokalizacji zdalnych na serwer FTP.
25. Możliwość przywrócenia backupu całego obrazu dysku/partycji na takim samym sprzęcie, jak ten który był backupowany jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników do nowego sprzętu lub możliwość dodania sterowników przez użytkownika. Komputer powinien zostać uruchomiony z bootowalnej płyty CD lub pendrive’a, z którego bezpośrednio zostaje uruchomiony proces odzyskiwania obrazu dysku z backupu.
26. Program pozwala na dowolne odtwarzanie maszyn fizycznych na inną fizyczną lub do maszyny wirtualnej, oraz z maszyny wirtualnej do innej maszyny wirtualnej lub na fizyczną.
27. Bez względu na rozmiar backupu, program umożliwia automatyczne uruchomienie systemu z backupu jako maszyny wirtualnej w środowiskach VirtualBox, VMware vSphere lub Hyper-V bez konieczności wcześniejszej konwersji pliku backupu do postaci wirtualnej.
28. Program umożliwia zamontowanie pliku backupu jako dysku wirtualnego w trybie odczyt/zapis lub tylko do odczytu. Tak podłączony dysk logiczny umożliwia przeglądanie, wyszukiwanie i odzyskiwanie plików, folderów a także modyfikowanie zawartości.
29. Podczas przywracania obrazu dysku/partycji z kopii zapasowej, program umożliwia: uaktywnienie wybranej partycji, przywrócenia sektora MBR, przywrócenie sygnatur dysku, przywrócenie ukrytych ścieżek na dysku, dezaktywację licencji systemu Windows.
30. Program pozwala na zdefiniowanie procesu tworzenia kolejnych backupów przyrostowych, które w sposób automatyczny będą odtwarzane po określonym przez administratora czasie na innej maszynie fizycznej lub wirtualnej (VMDK, VHD, VHDX). Musi istnieć możliwość zdefiniowania opóźnienia z jakim kopie przyrostowe będą przenoszone na nowy wolumin w zakresie od 1 godziny do 30 dni.
31. Program musi umożliwiać pełną konfigurację i pełne zarządzanie zadaniami wykonywania kopii zapasowej na innych komputerach w sieci lokalnej, w zakresie identycznym jak z lokalnej konsoli administracyjnej.
32. Musi być dostępne narzędzie dające możliwość tworzenia zadań backupu za pomocą polityk dla grup stacji z poziomu konsoli webowej.
33. Konsola webowa musi umożliwiać instalację oraz aktualizację zdalną oprogramowania na punktach końcowych.
34. Konsola webowa musi umożliwiać podgląd dzienników zdarzeń na stacjach końcowych.
35. Program musi umożliwiać wysłanie powiadomień w postaci wiadomości e-mail gdy: zadanie backupu zakończyło się niepowodzeniem, po zakończeniu zadania tworzenia backupu, oraz podsumowanie aktywności dziennej, tygodniowej i miesięcznej.

Musi istnieć możliwość pobrania ze strony producenta konsoli zarządzającej w postaci pliku ISO.

**Narzędzie do zarządzania logami 1 szt**

Wymagana jest obsługa różnych typów logów, w tym logów systemowych, aplikacyjnych, sieciowych, oraz logów bezpieczeństwa (np. zdarzenia związane z uwierzytelnianiem, ataki, itp.).

Urządzenie musi być skalowalne, aby obsłużyć obecne oraz przyszłe zapotrzebowanie na zbieranie i analizę logów. Musi umożliwiać łatwe dodawanie nowych źródeł logów oraz elastyczne zwiększanie mocy obliczeniowej i przestrzeni dyskowej w razie potrzeby.

Wsparcie dla protokołów bezpiecznej transmisji danych, w tym SSL/TLS, zapewniających szyfrowanie danych logów w transmisji.

Zapewnienie bezpieczeństwa danych logów poprzez mechanizmy uwierzytelniania, autoryzacji i szyfrowania, w celu zapobiegania nieautoryzowanemu dostępowi oraz zabezpieczenia przed utratą danych w razie awarii.

Możliwość integracji z istniejącymi systemami bezpieczeństwa IT, takimi jak rozwiązania antywirusowe, systemy wykrywania intruzów (IDS/IPS) oraz platformy zarządzania zdarzeniami bezpieczeństwa (SIEM), w celu zapewnienia kompleksowego monitorowania i ochrony infrastruktury.

Zapewnienie wsparcia dla elastycznych mechanizmów archiwizacji i retencji danych logów, umożliwiających przechowywanie danych zgodnie z wymaganiami regulacyjnymi oraz potrzebami biznesowymi.

Możliwość konfiguracji oraz monitorowania wydajności systemu, w tym zbierania statystyk dotyczących obciążenia, wykorzystania zasobów oraz przepustowości, w celu optymalizacji działania oraz planowania przyszłych wymagań infrastrukturalnych.

Wsparcie dla wielu formatów logów oraz umożliwienie elastycznego przetwarzania i analizy danych logów, w tym filtrowania, agregacji, normalizacji oraz tworzenia niestandardowych raportów i dashboardów.

**Urządzenia UPS do komputerów stacjonarnych 10 szt.**

**Dane techniczne**

|  |  |
| --- | --- |
| Rodzaj: | **wolnostojący** |
| Czas przełączania: | **6 ms** |
| Moc skuteczna: | **1200 W** |
| Moc pozorna: | **2000 VA** |
| Napięcie wyjściowe: | **230 V** |
|  |  |
| Kształt przebiegu sinusoidy: | **sinusoida modulowana** |
| Napięcie wejściowe: | **230 V** |
| Interfejs: | **USB, RJ-45** |
| Liczba gniazd wyjściowych: | **4** |
| Liczba gniazd Schuko: | **4** |
| Sygnalizacja pracy: | **diody LED, dźwiękowa** |
| Zabezpieczenia: | **przeciwprzepięciowe, przed przeładowaniem** |
| Typ akumulatora: | **2 x 12V/9Ah** |

**Serwery do wykonywania kopii bezpieczeństwa 2 szt**

Charakterystyka (wymagania minimalne)

**Obudowa**

Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.

**Płyta główna**

Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

Chipset Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

**Procesor**

Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 173 w teście

SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.

**RAM**

Minimum 256GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1.5TB pamięci RAM.

**Funkcjonalność pamięci RAM**

Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing

**Gniazda PCI**

Minimum jeden slot PCIe x16 generacji 4

**Interfejsy sieciowe/FC/SAS**

Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy

sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w

slotach PCIe)

**Dyski twarde**

Możliwość instalacji dysków SAS, SATA, SSD

Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB, 6Gb, 2,5“ Hot-Plug.

**Kontroler RAID**

Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10.

**Wbudowane porty**

3x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.

**Video**

Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200

**Zasilacze**

Redundantne, Hot-Plug min. 1100W każdy.

**Bezpieczeństwo**

* Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
* Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
* BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
* Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
* Moduł TPM 2.0
* Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera
* Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem

**Diagnostyka**

Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.

**Karta Zarządzania**

Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla IPv6;
* wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji
* sprzętowej.
* możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
* możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

**System operacyjny i licencje**

Windows Server 2022 Standard lub system równoważny. Licencjonowanie ma upoważniać do jednoczesnego uruchomienia czterech maszyn wirtualnych z system operacyjnym Windows Server 2022. Certyfikaty Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE.

**Warunki gwarancji**

3 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Możliwość rozszerzenia gwarancji przez producenta do 7 lat.

Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera

**Dokumentacja użytkownika**

Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

**Macierz serwerowa**

|  |  |
| --- | --- |
| **Parameter** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19”, macierz musi zajmować maksymalnie 2U i pozwalać na instalacje 12 dysków 3.5”. |
| **Kontrolery** | Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów 25Gb iSCSI |
| **Kable/wkładki** | Min. 1 kabel DAC SFP28 do SFP28, 25GbE, 1 metr długości |
| **Cache** | 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii. |
| **Dyski**  | Zainstalowane:6 dysków Hot-Plug o pojemności 1.92B SSD SAS, 24Gbs, 2,5’Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki. |
| **Oprogramowanie/Funkcjonalności** | Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz.Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków.Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 8TB poprzez dyski SSD. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym. |
| **Wsparcie dla systemów operacyjnych** | Windows Server 2022, Windows Server 2019, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi, Citrix XenServer |
| **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. |
| **Warunki gwarancji dla macierzy** | 3 lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygasnięcia gawarancji macierzy.* Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.
* Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu.
* W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
 |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim |
| **Certyfikaty** | Macierz musi być wyprodukowana zgodnie z normą ISO 9001:2015.  |

**Wdrożenia**

**Wdrożenie klastra serwerów wraz z zasilaniem awaryjnym**

1. Montaż zasilacza UPS w szafie rackowej
2. Konfiguracja podtrzymania awaryjnego
3. Konfiguracja iDRAC
4. Konfiguracja RAID z dysków w serwerze
5. Instalacja, aktywacja i aktualizacja systemu Windows Server 2022
6. Konfiguracja połączenia iSCSI z serwerem plików Dell
7. Konfiguracja agregacji łączy i wirtualnego przełącznika
8. Utworzenie roli Hyper-V
9. Konfiguracja funkcji wielościeżkowości do macierzy
10. Podłączenie serwerów do aktualnej domeny Active Directory
11. Utworzenie klastra z dwóch serwerów
12. Podłączenie macierzy dyskowej do klastra
13. Migracja czterech maszyn wirtualnych
14. Testy funkcjonalne

**Wdrożenie macierzy SAN**

1. Aktualizacja firmware
2. Konfiguracja RAID 6
3. Konfiguracja interfejsów sieciowych macierzy
4. Konfiguracja iSCSI macierzy
5. Konfiguracja agregacji łączy macierzy
6. Konfiguracja LUN
7. Testy funkcjonalne macierzy

**Segmentacja sieci z użyciem klastra UTM, dwóch przełączników dystrybucyjnych 8x8 oraz dwóch przełączników 48p**

1. Montaż przełączników dystrybucyjnych w miejscu wyznaczonym przez zamawiającego
2. Podstawowa konfiguracja przełączników dystrybucyjnych
3. Konfiguracja interfejsów sieciowych przełączników dystrybucyjnych
4. Konfiguracja agregacji łączy na wybranych portach
5. Montaż przełączników dostępowych
6. Podstawowa konfiguracja przełączników dostępowych
7. Konfiguracja interfejsów sieciowych przełączników dostępowych
8. Konfiguracja przełączników do pracy w trybie jednej grupy logicznej
9. Podłączenie przełączników dostępowych do przełączników
10. Montaż i instalacja obu urządzeń UTM
11. Konfiguracja interfejsów sieciowych UTM
12. Odtworzenie konfiguracji obecnego UTM
13. Konfiguracja obu UTM do pracy w trybie klastra wysokiej dostępności
14. Konfiguracja klastra UTM do świadczenia usługi routingu w obrębie segmentów sieci
15. Zdefiniowanie reguł klastra UTM w obrębie segmentowanej sieci
16. Zdefiniowanie reguł firewall w zakresie komunikacji między urządzeniami końcowymi
17. Testy funkcjonalne
18. Wdrożenie ma być wykonywane przez inżynierów posiadających certyfikaty z oferowanych rozwiązań.

**Wdrożenie** **oprogramowania do tworzenia i zarządzania kopiami bezpieczeństwa na dwóch maszynach wirtualnych i sześciu stacjach roboczych**

1. Instalacja oprogramowania na urządzeniach końcowych
2. Konfiguracja miejsca docelowego dla backupu urządzeń końcowych
3. Stworzenie harmonogramu backupu na urządzeniach końcowych
4. Instalacja konsoli zarządzającej na serwerze plików
5. Integracja konsoli zarządzającej z oprogramowaniem zainstalowanym na urządzeniach końcowych
6. Konfiguracja oprogramowania zgodnie z wymaganiami zamawiającego
7. Testy funkcjonalne
8. Wdrożenie ma być wykonywane przez inżynierów posiadających certyfikaty z oferowanych rozwiązań.

**Wdrożenie** **serwera plików do przechowywania kopii zapasowych**

1. Aktualizacja firmware
2. Konfiguracja RAID 6
3. Konfiguracja ustawień sieciowych
4. Konfiguracja iSCSI
5. Instalacja oprogramowania do kopii bezpieczeństwa
6. Konfiguracja oprogramowania do kopii bezpieczeństwa w celu zarządzania zreplikowanymi danymi
7. Utworzenie miejsca docelowego backupu na wdrożonej macierzy NAS
8. Utworzenie zadań backupu
9. Testy funkcjonalne

**Wdrożenie narzędzia do zarządzania logami**

1. Analiza infrastruktury generującej logi
2. Instalacja i konfiguracja źródeł logów
3. Uruchomienie filtrów i reguł przetwarzających logi
4. Konfiguracja harmonogramów przetwarzania logów
5. Konfiguracja monitorowania oraz alarmowania
6. Konfiguracja raportowania
7. Testy funkcjonalne

**Szkolenie specjalistyczne dla informatyków**

**Zakres szkolenia UTM – ogólny:**

1. Omówienie roli UTM w infrastrukturach sieciowo-serwerowych
2. Omówienie interfejsu UTM
3. Podstawowa konfiguracja ustawień systemowych i aktualizacji
4. Omówienie konfiguracji interfejsów sieciowych do świadczenia usługi routingu
5. Omówienie konfiguracji UTM do świadczenia usług serwera DHCP
6. Tworzenie i zarządzanie regułami firewall zgodnie z dobrymi praktykami zabezpieczeń
7. Omówienie integralności z systemami autoryzacji
8. Omówienie idei oraz konfiguracji klastra UTM
9. Omówienie zaawansowanych opcji – VPN, IPS
10. Omówienie ochrony przed złośliwym oprogramowaniem (DPI, repozytoria sygnatur wirusów)
11. Omówienie skalowalności rozwiązania w kontekście wykorzystania rozwiązań UTM

**Zakres szkolenia oprogramowania do tworzenia i zarządzania kopiami bezpieczeństwa**

1. Instalacja oprogramowania w najnowszej wersji
2. Omówienie agenta oraz jego funkcjonalności
3. Tworzenie miejsc docelowych dla backupu
4. Stworzenie zadania z uwzględnieniem dostępnych opcji
5. Omówienie przywracania danych
6. Odzyskiwanie selektywnych plików
7. Praktyczne zastosowanie narzędzi dostępnych w oprogramowaniu
8. Odtworzenie środowiska za pomocą oprogramowania

**Zakres szkolenia z zarządzania przełącznikami wielowarstwowymi**

1. Idea zastosowania przełączników zarządzalnych L2/L3 w kontekście cyberbezpieczeństwa
2. Segmentacja sieci, a skuteczne zarządzanie infrastrukturą sieciowo-serwerową
3. Interfejsy oraz funkcje wykorzystywane w przełącznikach
4. Omówienie funkcji agregacji połączeń
5. Omówienie funkcji raportowania syslog oraz SNMPv2 trap
6. Omówienie interfejsu konsoli zarządzania przełącznika
7. Omówienie konfiguracji i zastosowania wirtualnych sieci lokalnych
8. Omówienie koncepcji VLAN
9. Omówienie idei wykorzystania UTM lub przełączników warstwy 3 do routingu w wirtualnych sieciach lokalnych

**Zakres szkolenia z serwera NAS**

1. Idea zastosowania serwera plików i macierzy dyskowych
2. Integracja z active directory
3. Omówienie rodzajów wykorzystywanych protokołów
4. Omówienie sposobu działania i funkcjonalności RAID 0,1,5,6
5. Omówienie konfiguracji interfejsu sieciowego
6. Omówienie współdzielenia plików oraz mapowania dysków
7. Funkcje cyberbezpieczeństwa w serwerach NAS
8. Omówienie zabezpieczeń maszyn wirtualnych