Znak Funduszy Europejskich (FE) 
złożony z symbolu graficznego, nazwy Fundusze Europejskie oraz nazwy programu, z którego w części lub w całości finansowany jest  projekt
Znak barw Rzeczypospolitej Polskiej (znak barw RP) 
złożony z barw RP oraz nazwy „Rzeczpospolita Polska”
Znak godło Województwa Świętokrzyskiego
Znak Unii Europejskiej (UE) 
złożony z flagi UE, napisu Unia Europejska i nazwy funduszu, który współfinansuje projekt 

**Modernizacja serwerowni w budynku Biobanku Regionalnego Centrum Naukowo Technologicznego w Podzamczu**

**Szczegółowy opis przedmiotu zamówienia**

1. Serwer produkcyjny - 2szt.

2 Macierz dyskowa – 1 szt.

3. System bezpieczeństwa – 1 szt

4. Oprogramowania do monitorowania i nadzorowania sieci – 1szt

5. Migracja środowiska produkcyjnego – 1 szt

Szczegółowy opis komponentów:

1. **Serwer produkcyjny.**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |  |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5" Hot-Plug wraz z kompletem szyn umożliwiających montaż w szafie rack. Organizer kablowy nie jest wymagany.  Dodatkowo obudowa musi być wyposażona w maskownicę, chroniącą dyski przed nieuprawnionym dostępem fizycznym.  Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |  |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| **Chipset** | Dedykowany przez producenta procesor do pracy w serwerach dwuprocesorowych |  |
| **Procesor** | Zainstalowane dwa procesory ośmio-rdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem.  Procesor umożliwiający osiągnięcie wyniku min. 11219 punktów w teście High End CPUs dostępnym na stronie <https://www.cpubenchmark.net/> |  |
| **RAM** | 256GB DDR4 RDIMM 3200MT/s w modułach 32GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. |  |
| **Gniazda PCIe** | Min. 1 x PCIe Gen 3 o prędkości x16 pełnej wysokości |  |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror |  |
| **Interfejsy sieciowe/FC** | Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T, nie zajmujące slotów PCIe.  Dodatkowo zainstalowana karta czteroportowa 10GbE w standardzie Base-T. |  |
| **Napęd optyczny** | DVD RW |  |
| **Wewnętrzna pamięć masowa** | Dwa dyski twarde o pojemności minimum 1 TB 7,2k SATA typu hot-lug |  |
| **Kontroler RAID** | Wyposażony w minimum 8 GB pamięci cache z obsługa grup RAID: 0,1,5,6,10,50,60 |  |
| **Wbudowane porty** | Min. 4 porty USB, w tym min. 1 port USB 2.0 z przodu serwera. 2 porty USB 3.0 z tyłu serwera oraz 1 wewnętrzny port USB 3.0.  Dedykowany port micro-USB służący do komunikacji z system zarządzającym serwera  2 porty RJ45, 2 port VGA, min. 1 port RS232. |  |
| **Wentylatory** | Redundantne |  |
| **Zasilacze** | Redundantne, Hot-Plug maksymalnie 550W.  Dodatkowo dwa kable zasilające z wtykami C13/C14 o dł. min. 2m. |  |
| **Bezpieczeństwo** | Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  Moduł TPM nie jest wymagany. |  |
| **System operacyjny** | Nie jest wymagany |  |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * 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 SNMP; IPMI2.0, VLAN tagging, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * możliwość obsługi przez dwóch administratorów jednocześnie * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232. * możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. * monitorowanie zużycia dysków SSD * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, * automatyczne zgłaszanie alertów do centrum serwisowego producenta * automatyczne update firmware dla wszystkich komponentów serwera * możliwość przywrócenia poprzednich wersji firmware   Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:   * możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * szczegółowy opis wykrytych systemów oraz ich komponentów * możliwość eksportu raportu do CSV, HTML, XLS, PDF * możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. * grupowanie urządzeń w oparciu o kryteria użytkownika * możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * szybki podgląd stanu środowiska * podsumowanie stanu dla każdego urządzenia * szczegółowy status urządzenia/elementu/komponentu * generowanie alertów przy zmianie stanu urządzenia. * filtry raportów umożliwiające podgląd najważniejszych zdarzeń * kreator umożliwiający dostosowanie akcji dla wybranych alertów * możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów * aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta * możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. * dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. * oprogramowanie dostarczane jako wirtualny appliance dla ESXi i Hyper-V. |  |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001:2015. |  |
| **Warunki gwarancji** | Pięć lat 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. |  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |  |

1. **Macierz dyskowa**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa parametru** | **Minimalna wartość parametru** |
|  | Obudowa | System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. |
|  | Pojemność: | System musi zostać dostarczony w konfiguracji zawierającej minimum  11 dysków 800GB SSD  i zajmować maksymalnie 2U w szafie rack  System musi ponadto wspierać dyski:  - SSD: od 800GB do 15.3TB  System musi mieć możliwość rozbudowy do minimum 90 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. |
|  | Kontroler | 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.  System musi pozwalać na rozbudowę do 32GB pamięci cache na kontroler |
|  | Interfejsy | Oferowana macierz musi posiadać minimum  - 4 porty 10GbE RJ45 do podłączenia hostów  - 4 porty SAS 12 Gb/s do podłączenia półek dyskowych  oraz pozwalać na rozbudowę o dodatkowe 8 portów 16Gb FC/10GbE SFP+ do podłączenia hostów. |
|  | 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. |
|  | Obsługiwane protokoły | FC, iSCSI , SAS oraz CIFS i NFS  Technologia macierzy w przypadku rozbudowy o porty FC musi pozwalać na zmianę udostępniania danych z FC na iSCSI i na odwrót bez zmiany wkładek SFP+. Zamawiający pozwala na dostarczenie macierzy, która nie spełnia tego warunku przy założeniu zaoferowania rozwiązania od razu wyposażonego w:  12 portów FC 16Gb  12 portów 10GbE SFP+  Realizację protokołu CIFS i NFS zamawiający dopuszcza za pomocą zewnętrznego oprogramowania software define Storage innego producenta niż macierz. |
|  | 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, system musi pozwalać na wykonanie do 30 jednoczesnych replikacji.  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 120 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  - Vmware SRM  - MicrosoftVirtual 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 Define 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. Szyfrowanie musi być dostępne za pomocą dysków samoszyfrujących lub dedukowanego oprogramowania dla zasobu NAS. |
|  | Gwarancja i serwis | 5 lat 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 5 lat subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. |

1. **System bezpieczeństwa**

# **Wymagania ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

# **Funkcje modułu Firewall**

1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2. System realizujący funkcję Firewall musi zostać dostarczony w postaci klastra pracującego w trybie Active-Passive składającego się z dwóch urządzeń fizycznych.
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Urządzenie musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.
28. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego

agenta na stacjach roboczych użytkowników.

1. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
2. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
3. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
4. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
5. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
6. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
7. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
8. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
9. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
10. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
11. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
12. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

# **Dostarczony system bezpieczeństwa musi zapewniać:**

1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed nieznanymi zagrożeniami.
4. Ochronę przed phishingiem.
5. Ochronę przed niechcianą pocztą.
6. Kontrolę wykorzystywanych aplikacji.
7. Możliwość filtrowania URL.

# **Parametry fizyczne systemu Firewall:**

Element systemu pełniący funkcję Firewall musi dysponować :

* 8 portami 1Gb RJ45 w tym 2 porty obsługujące standard PoE+ (802.3at).
* Możliwość rozbudowy urządzenia o dodatkowy port 10Gb SFP+.
* Wbudowany dysk SSD o pojemności 128GB.
* Minimum 4 GB pamięci RAM.
* Minimum 2 porty USB 3.0.
* Minimum jeden port typu Console.
* Minimalna temperatura pracy urządzenia od 0 do 40 stopni Celsjusza.

# **Parametry wydajnościowe systemu:**

* Przepustowość Firewall minimum: 4.7 Gbps.
* Przepustowość IPSec VPN nie mniejsza niż: 1.4 Gbps.
* Przepustowość skanowania antywirusowego nie mniejsza niż: 1.1 Gbps.
* Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 909 Mbps.
* Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 631 Mbps.
* Obsługa nie mniej niż: 60 tuneli IPSec site-to-site.
* Obsługa nie mniej niż: 60 tuneli client-to-site.
* Obsługa nie mniej niż: 500.000 jednoczesnych połączeń.
* Obsługa nie mniej niż: 25.000 nowych połączeń na sekundę.
* W ramach Firewall system musi obsługiwać minimum: 75 sieci VLAN.

# **W ramach ochrony przed atakami system musi zapewniać:**

1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

# **W ramach kontroli antywirusowej system musi zapewniać:**

1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.
2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

# **W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać:**

1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję analizy behawioralnej w oparciu o platformę typu sandbox, w tym co najmniej:

* W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej).
* Analizę plików pobieranych przez HTTP/HTTPS i przesyłanych pocztą elektroniczną (SMTP, POP3, IMAP) oraz plików pobieranych za pomocą protokołu FTP.
* Ogólne oszacowanie poziomu ryzyka dla analizowanych plików i określanie różnego rodzaju akcji na ich podstawie.
* Kwarantannę podejrzanych plików co najmniej dla protokołu SMTP.
* Możliwość blokowania wiadomości e-mail przesyłanej protokołem SMTP zawierającej podejrzane załączniki do czasu zakończenia ich analizy.
* Możliwość analizy plików o rozmiarze co najmniej 10MB.
* Brak ograniczeń co do ilości analizowanych plików.

# **W ramach ochrony przed phishingiem system musi zapewniać:**

1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję ochrony przed phishingiem, w tym co najmniej:

* Możliwość blokowania dostępu do spreparowanych stron.
* Ochronę przed phishingiem nie zależnie od typu połączenia, protokołu, portu.
* Możliwość tworzenia białych/czarnych list domen, do których połączenia będą filtrowanie.
* Notyfikację użytkownika, którego dotyczy zdarzenie - niezależnie od logów i raportów.
* Kontrolę zapytań DNS.

# **W ramach kontroli antyspamowej system musi zapewniać:**

1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.
6. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

# **W ramach filtrowania zawartości URL system musi zapewniać:**

1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
8. Możliwość określania reputacji adresu URL i na podstawie reputacji podejmowanie określonych akcji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu https.
13. Wyłączenie inspekcji https dla wybranych kategorii stron www.

# **W ramach kontroli aplikacyjnej system musi zapewniać:**

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1800, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
5. Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji.

# **Wymagane funkcje VPN systemu:**

1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
13. Musi umożliwiać uruchomienie portalu SSL VPN, który umożliwia autoryzację w oparciu o protokoły RADIUS, LDAP, Active Directory, lokalną bazę użytkowników.
14. Portal SSL VPN musi zapewniać wsparcie dla protokołów: SSH, RDP, HTTP.
15. Portal SSL VPN musi wspierać funkcjonalność Single-Sign-On dla aplikacji webowych w oparciu o protokół SAML.

# **Zarządzanie**

1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

# **Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:**

1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
8. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
9. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
10. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
11. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
12. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
13. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
14. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
15. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
16. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
17. System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
18. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
19. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
20. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
21. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
22. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
23. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

# **Licencje i wsparcie techniczne**

1. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:

* Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów, Rozpoznawanie urządzeń pracujących w sieci, Ochrona przed nieznanymi zagrożeniami, Ochrona przed phishingiem, – na okres 5 lat.

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 5 lat, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 (świadczone telefonicznie lub poprzez portal).
2. **Oprogramowania do monitorowania i nadzorowania sieci**

**Dostawa licencji oprogramowania do monitorowania i nadzorowania sieci. Oprogramowanie to powinno posiadać następującą charakterystykę:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Szczegółowy zakres przedmiotu zamówienia wymagany przez Zamawiającego** |  |
| 1 | Wymogi ogólne:   1. Oprogramowanie powinno posiadać budowę modułową i składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu (TLS lub SSL). Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomoc w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows. 2. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Powinny one być również grupowane w osobnym, dedykowanym oknie, aby możliwe było, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. 3. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, powinien być objęty kontrolą na poziomie wybranych Administratorów – w programie powinna być możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników. **Działania administratorów powinny być logowane oznacza to, że program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie.** 4. **Oprogramowanie powinno posiadać obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety powinny móc być rozłożone na siatce o rozmiarze ustalonym przez administratora. Obszar pozwala na wyświetlanie danych z całego systemu.** 5. **Oprogamowanie powinno umożliwiać zarządzanie przynajmniej 50 stacjami roboczymi** | |
| 2 | Program powinien być dostępny w języku polskim i angielskim wraz z podręcznikiem użytkownika w formie strony internetowej. Należy podać link do strony zawierającej podręcznik użytkownika. |  |
| 3 | **Serwer bazy danych, na której działają wszystkie oferowane moduły powinien umożliwiać pracę dla nieograniczonej ilości użytkowników oraz nielimitowanej pojemności bazy. Należy wskazać nazwę bazy danych dla oferowanego rozwiązania uwzględniając powyższe wymogi.** |  |
| 4 | Wymogi dotyczące poszczególnych funkcji |  |
|  | 1. MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:  * wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping). * wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci. * **wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.** * wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków * serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów. * **zablokowania mapy urządzeń przed przypadkową edycją.** * serwerów pocztowych:   + program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę,   + program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),   + program powinien posiadać możliwość wykonywania operacji testowych,   + program powinien wysyłać powiadomienia, jeśli serwer pocztowy nie działa. * monitorowania serwerów WWW i adresów URL. * **obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.** * **obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) za pomocą nazw.** * **szyfrowania AES, DES i 3DES dla protokołu SNMPv3**, * **obsługi komunikatów syslog, pułapek SNMP i ewidencjonowanie odebranych z nich danych**, * monitoringu routerów i przełączników wg:   + zmian stanu interfejsów sieciowych,   + ruchu sieciowego,   + podłączonych stacji roboczych,   + ruchu generowanego przez podłączone stacje robocze * **Program powinien posiadać własny, wbudowany kompilator plików MIB umożliwiający dodawanie definicji dla modułów SNMP** * serwisów Windows: monitor serwisów Windows powinien informować gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie. * wydajności systemów Windows:   + obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.   Program powinien posiadać Inteligentne Mapy i Oddziały/Jednostki organizacyjne, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały/Jednostki organizacyjne) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). |  |
|  | 1. INWENTARYZACJA - program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:  * Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. * Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. * Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows, co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. * Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. * Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. * Umożliwiać odczytanie numeru seryjnego (klucze licencyjne). * Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. * Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. * **Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 10.** * **Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.**   Moduł inwentaryzacji sprzętu powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie:   * przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, * definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości – dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo powinien istnieć możliwość importu danych z zewnętrznego źródła (.CSV), * generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania, * archiwizacji i porównywania audytów środków trwałych, * tworzenia kodów kreskowych w Środkach Trwałych, * drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy, * inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej na system Android, * inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline). * określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, * określenia atrybutów dodatkowych tylko dla wybranych typów zasobów * definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,   Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:   * Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. * Informacje o aplikacjach używanych w organizacji. * Tworzenie własnych wzorców aplikacji. * Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. * Informacje o komputerach, na których aplikacja została wykryta. * Zarządzanie posiadanymi licencjami. * **Wskazywanie osób odpowiedzialnych za licencję.** * Wskazanie użytkowników licencji. * **Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10.** * **Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.** * Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. * Zarządzanie posiadanymi licencjami: raport zgodności licencji. Możliwość przypisania do programów numerów seryjnych, wartości itp.   Okna audytowe powinny posiadać możliwość filtrowania elementów per jednostka organizacyjna |  |
|  | 1. OBSŁUGA UŻYTKOWNIKÓW- program powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:  * Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy) * Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz z informacją o uruchomieniu na podwyższonych uprawnieniach, * Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona), * Informacji o edytowanych przez użytkownika dokumentach, * Historii pracy (cykliczne zrzuty ekranowe), * Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt), * Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), * Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program powinien mieć możliwość monitorowania kosztów wydruków, * Nagłówków przesyłanej poczty e-mail.   Program ponadto powinien posiadać możliwość:   * blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl), * blokowania ruchu na wskazanych portach TCP/IP, * blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, * wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. * definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.   Program powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które będą służyć do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych. |  |
|  | 1. Moduł wydajności czasu pracy – program powinien wspierać zarządzanie czasem i analizować aktywność użytkowników poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. System powinien umożliwić każdemu pracownikowi organizacji dostęp do własnych wskaźników aktywności. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania.   Dodatkowo moduł gromadzi oraz prezentuje w formie strony www:   * Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. * Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy. * Statystyki aktywności podwładnych widoczne dla przełożonego. * Listy odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. * Podglądy list użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. * Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. * Oceny produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. * Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.  1. ZDALNA POMOC UŻYTKOWNIKOM - w ramach kontroli stacji użytkownika powinien być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu będzie mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika.   W niniejszym module musi znaleźć się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei będą przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Użytkownik powinien mieć możliwość monitorowania procesu rozwiązywania zgłoszonych problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które będą wpisywane i widoczne dla obu stron. Moduł ten powinien zawierać również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy.  Moduł pomocy zdalnej będzie umożliwiać również:   * pobieranie listy użytkowników z Active Directory, * **zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,** * **zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej,** * tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), * automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, * procesowanie zgłoszeń użytkowników z wiadomości e-mail, * **tworzenie formularzy z niestandardowymi polami opisowymi**, dedykowanymi do wybranych kategorii zgłoszeń, * wykonywanie operacji na wielu zgłoszeniach równocześnie, * dołączanie załączników do zgłoszeń, * rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, * szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, * **wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,** * zrzuty ekranowe (podgląd pulpitu), * dystrybucję oprogramowania przez Agenty, * dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), * zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, * **zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),** * **wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików** |  |
|  | 1. OCHRONA DANYCH – powinna odbywać się poprzez blokowanie następujących urządzeń:  * Blokowanie urządzeń i nośników danych. Program powinien mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. * Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. * Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. * Blokownie powinno dotyczyć tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.   Zarządzanie prawami dostępu do urządzeń powinien odbywać się poprzez:   * Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. * Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane. * Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. * Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.   Audyt operacji na urządzeniach przenośnych będzie odbywać się poprzez:   * Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. * Podłączenie/odłączenie urządzenia przenośnego.   System umożliwia monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.  Integracja z Active Directory powinna odbywać się poprzez zarządzanie prawami dostępu przypisanymi do użytkowników grup domenowych. Przydzielanie uprawnień będzie powinno być możliwe również do kont użytkowników lokalnych.  Ochrona przed usunięciem - program powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora.  Program WSPIERA ZARZĄDZANIE CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może uzyskać dostęp do własnych wskaźników aktywności. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. 1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy. 3. Statystyki aktywności podwładnych widoczne dla przełożonego. 4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. 5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. 6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. 7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. 8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. 10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 11. Wskaźnik czasu poświęconego na aktywność produktywną. 12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji. 14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji. |  |
| 5 | **Program powinien być objęty gwarancją producenta w okresie min 5 lat od czasu wdrożenia** |  |

1. **Migracja środowiska produkcyjnego**

Migracja obecnego środowiska na nowe serwery oraz macierze w tym:

Migracja kontrolerów domeny wraz podniesieniem systemów operacyjnych serwerów do wersji Windows Server 2019.

Instalacja i konfiguracja serwerów. Fizyczny montaż pierwsze uruchomienie instalacja najnowszych firmware.

Instalacja systemów operacyjnych sterowników i poprawek.

Uruchomienia Hypervisora Hyper-V na windows Server 2019.

Instalacja i konfiguracja Macierzy Dyskowej. Fizyczny montaż pierwsze uruchomienie instalacja najnowszego firmware.

Utworzenie LUN pod wirtualne maszyny oraz konfiguracja z nowo zainstalowanymi serwerami

Migracja maszyn wirtualnych na nowy hypervisor oraz storage.

Migracja serwera plików.

Migracja serwera DHCP.

Migracja Serwera DNS.

Uruchomienie roli serwera do zarządzania poprawkami dla systemów Windows.

Konfiguracja sieci oraz firewall zgodnie z wymogami zamawiającego.

Konfiguracja sieci WAN oraz LAN

Konfiguracja VPN dla użytkowników przez protokół SSL

Integracja z usługą Active Directory

Uruchomienie funkcjonalności IDS/IPS, Gateway AV

Przepisanie reguł firewall i ustawień customowych z obecnego rozwiązania Zyxell USG

Konfiguracja kopii zapasowej dla całego środowiska wraz z urządzeniami aktywnymi.

Instalacja i konfiguracja aplikacji do zarządzania siecią oraz stacjami roboczymi.

Przeszkolenie administratora zamawiającego z głównie z obsługi środowiska systemowego oraz aplikacji do zarządzania i firewalla. Szkolenie zdalnie lub w siedzibie zamawiającego. Szkolenie nie krótsze niż 6 godzin.