Spis treści

[1. Przełącznik rdzeniowy 2](#_Toc173315161)

[2. System kontroli dostępu do sieci (NAC) 5](#_Toc173315162)

[3. Przełącznik dostępowy 8](#_Toc173315163)

[4. System bezpieczeństwa sieci NGFW (UTM) 10](#_Toc173315164)

[a. Serwer pocztowy raz z systemem ochrony poczty internetowej 22](#_Toc173315165)

[6. Serwery pod wirtualizację 28](#_Toc173315166)

[7. Macierz dyskowa 33](#_Toc173315167)

[8. Serwer backup 37](#_Toc173315168)

[9. Biblioteka taśmowa 41](#_Toc173315169)

[10. Oprogramowanie do wirtualizacji 43](#_Toc173315170)

[11. Oprogramowanie do backupu 45](#_Toc173315171)

[12. Wdrożenie wszystkich powyższych punktów 49](#_Toc173315172)

# Przełącznik rdzeniowy

2 sztuki

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Typ  | Przełącznik sieciowy zarządzalny rack SFP+. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
| Porty  | 1. Minimum 24 porty 1G/10G SFP+
2. Minimum 4 porty SFP56 z możliwością pracy 1G/10G/25G/50Gbit
3. Port konsoli – RS232 on USB typ C
4. Minimum 1 port USB typu A
5. Minimum 1 Bluetooth dongle
6. Port zarządzanie OOBM

Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, oraz Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX/LHCo najmniej 4 porty (typu uplink) SFP56 muszą umożliwiać ich obsadzanie wkładkami SFP28 Gigabit Ethernet, SFP+ 10Gbit oraz SFP 1Gbit a także kablami DAC 50Gbit.Możliwość łączenia w stos do 10 przełączników z wykorzystaniem uplinków, łączną przepustowość stosu do 200 GB/s na przełącznik. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. |
| Parametry fizyczne | Wysokość maksymalnie 1U, montowany w szafie typu rack 19’’, redundantny zasilacz |
| Pamięć | Co najmniej 8GB pamięci DDR4 Co najmniej 32GB pamięci flash |
| Wielkość tablicy adresów MAC | Co najmniej 32 000 |
| Ilość obsługiwanych sieci VLAN | Co najmniej 4094 |
| Wydajność  | * Przepustowość przełączania: min. 880 Gbit/s
* Przełączanie dla pakietów: min. 654 Mpps.
* Bufor pakietów: minimum 7.5 MB
* IPv4 multicast routers: 8192
* IPv4 unicast routers: 61000
* IPv6 Unicast Routes 60000
* IPv6 Multicast Routes 8000
 |
| Obsługa ramek Jumbo | O wielkości co najmniej 9198 bajtów |
| Funkcjonalność urządzenia | * + obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad),
	+ Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie
	+ wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree,
	+ Obsługa sFlow lub Netflow
	+ Obsługa skryptów w języku Python
	+ Obsługa REST API
	+ musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB,
	+ musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli,
	+ musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN
	+ plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.
	+ Obsługa 4000 jednoczesnych sieci VLAN 802.1Q
	+ Obsługa standardu 802.1v
	+ Obsługa protokołu MVRP
	+ Obsługa Ethernet Ring Protection Switching (ERPS)
	+ Wsparcie dla VXLAN
	+ Obsługa Microsoft Network Load Balancer (NLB)
	+ Obsługa SNTPv4 lub NTP
	+ Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
	+ Obsługa protokołów rutingu: ruting statyczny, RIPv2, RIPng, OSPF, OSPFv3, BGP, MP-BGP,
	+ Obsłyga ruchu multicast: IGMPv1/v2/v3, PIM-SM, PIM-DM, MSDP
	+ Obsługa VRRP
	+ Obsługa ECMP
	+ Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
	+ Wbudowany serwer DHCP
	+ Obsługa funkcji User Datagram Protocol (UDP) helper
 |
| Bezpieczeństwo | * + autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL,
	+ możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
	+ możliwość uzyskania dostępu do urządzenia przez SNMP, SSH, HTTPS z wykorzystaniem IPv4 i IPv6,
	+ obsługa mechanizmów Port Security, Dynamic ARP Inspection
	+ Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne).
 |
| Wsparcie dla mechanizmów zapewnienia jakość usług w sieci | * + klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie co najmniej następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
	+ implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Deficit Weighted Round Robin lub podobnego dla obsługi tych kolejek,
	+ możliwość obsługi jednej z powyżej wymienionych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
	+ możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi.
 |
| Zasilanie | Zasilacz 230V AC wymieniany hot-swap.Możliwość zastosowania redundantnego zasilacza wewnętrznego także hot-swap,Switch należy dostarczyć razem z dodatkowym zasilaczem redundantnym.Przełącznik dodatkowo powinien posiadać wentylację wymienną redundantną w postaci modułów hot-swap. |
| Akcesoria | Razem z przełącznikami należy dostarczy:* + - 1. Kabel DAC 50Gbit o długości m.in. 0,5m do zestawienia stack
 |
| Gwarancja | Dożywotnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory), obowiązując tak długo jak produkt jest oferowany przez producenta + 5 lat od momentu zakończenia produkcji.Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |
| Dokumenty | Wykonawca winien przedłożyć dokumenty:1. Deklaracja zgodności CE oferowanego urządzenia – certyfikat potwierdzony za zgodność z oryginałem,
2. Oświadczenie producenta lub oświadczenie autoryzowanego przedstawiciela producenta potwierdzające zgodność wszystkich parametrów oferowanego urządzenia wskazanych w Opisie przedmiotu zamówienia.
 |

# System kontroli dostępu do sieci (NAC)

1 sztuka

System do kontroli dostępu musi charakteryzować się następującymi cechami:

* Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
* System musi odsługiwać minimum 500 urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia
* Praca jako maszyna wirtualna
* Musi posiadać wbudowany serwer Radius oraz TACACS +
* Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:
* Cisco Systems
* Fortinet
* Microsoft
* Alcatel-lucent Enterprise
* Aruba Networks
* Huawei
* Extreme Networks
* PaloAlto
* Producenta urządzeń sieciowych opisanych w tym postępowaniu
* System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.
* System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.
* Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
* Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych
* Microsoft Active Directory
* Radius
* Kerberos
* LDAP
* ODBC
* Współpraca z serwerami tokenów
* Musi obsługiwać metody profilowania
* DHCP
* TCP
* MAC OUI
* SNMP
* Cisco device sensor
* Wspierać protokoły
* Radius, Radius CoA, TACACS +, web authentication, SAML v2.0
* EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
* PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
* TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
* EAP-TLS
* PAP, CHAP, MSCHAPv1 i v2, EAP-MD5
* NAC, Microsoft NAP
* Windows machine authentication
* MAC Auth
* Audit (role oparte na porcie oraz skanowanie podatności)
* OCSP (Online Certificate Status Protocol)
* SNMP generic MIB, SNMP private MIB
* CEF (Common Event Format), LEEF (Log Event Extended Format)
* TLS 1.2
* Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami
* Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:
* Co najmniej ESX 4.0, ESXi 4.1 do 6.0
* Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise

- Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich. Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.

System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności

* Samodzielna rejestracja klientów gościnnych w oparciu o:
* Adres e-mail
* Numer telefonu (wiadomość SMS)
* Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
* Logowanie w oparciu o portale społecznościowe
* Funkcja integracji z systemami trzecimi poprzez API
* Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową
* Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
* Funkcja personalizacji strony gościnnej

- Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

* Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT
* System musi wspierać obsługę następujących systemów operacyjnych
* MS Windows
* Mac OS X
* iOS
* Android
* Ubuntu
* Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
* Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej
* Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
* Funkcja tworzenia unikalnych cerftyfikatów dla urządzeń.
* Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń
* Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID

- Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

System kontroli końcówek klienckich musi mieć następujące funkcjonalności

* System musi wspierać następujące systemy operacyjne
* Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)
* Apple Mac OS X 10.7 i nowsze
* Red HAT Enterprise Linux 4 i nowsze
* CentOS  4 (Community Enterprise Operating System) i nowsze
* Fedora Core 5 i nowsze
* SUSE linux 10.x i nowsze
* Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall
* Wyświetlanie informacji on-line o statusie monitorowanych końcówek
* System powinien obsługiwać agenta w formie
* Stałej (Presistent Agent)
* Tymczasowej (Dissolvabe Agent)
* Agenta NAP

- Zaoferowane rozwiązanie musi być uznane przez firmę analityczną Gartner Research. To znaczy, że musi być wymienione w bieżącym na moment składania oferty raporcie Market Guide for Network Access Control lub musi być wymienione w Gartner Peer Insights w kategorii Network Access Control.

- Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

- Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.

- Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu

Testy

- Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.

# Przełącznik dostępowy

8 sztuk

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Typ  | Przełącznik sieciowy zarządzalny rack. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
| Porty  | Minimum 24 porty 10/100/1000 BaseT z wsparciem dla standardów PoE (standardy 802.3af i 802.3at), umieszczone z przodu obudowy Minimum 4 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowyDedykowany port konsoli USBPort USB 2.0 (niezależny od portu konsoli USB) |
| Parametry fizyczne | Wysokość maksymalnie 1U, montowany w szafie typu rack 19’’ |
| Pamięć | Minimum 4GB pamięci operacyjnejMinimum 16GB wewnętrznej pamięci nieulotnej typu Flash. |
| Wielkość tablicy adresów MAC | Co najmniej 8000 |
| Ilość obsługiwanych sieci VLAN | Obsługa 4094 tagów IEEE 802.1Q oraz 512 jednoczesnych sieci VLAN |
| Wydajność  | * Przepustowość: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
* Wydajność: minimum 95 Mp/s
* Bufor pakietów: minimum 12 MB
* Wielkość tablicy routingu: minimum 500 wpisów IPv4, 500 wpisów IPv6
* Wielkość tablicy ARP co najmniej 1000 wpisów, wielkość tablicy ND co najmniej 500 wpisów
 |
| Obsługa ramek Jumbo | O wielkości co najmniej 9198 bajtów |
| Funkcjonalność urządzenia | * Obsługa sFlow lub Netflow
* Obsługa REST API
* Obsługa RMON (minimum grupy 1,2,3 i 9)
* Obsługa protokołu MVRP
* Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
* Obsługa Secure FTP lub SCP
* Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
* Obsługa SNTPv4 lub NTP
* Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping)
* Obsługa protokołów rutingu: ruting statyczny
* Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 500 grup), MLD (co najmniej 500 grup)
* Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
 |
| Bezpieczeństwo | * Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3
* Obsługa uwierzytelniania użytkowników zgodna z 802.1x
* Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
* Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
* Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
* Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
* Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
* Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
* Obsługa list kontroli dostępu (ACL)
 |
| Wsparcie dla mechanizmów zapewnienia jakość usług w sieci | Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting |
| Zasilanie | Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W. Pobór mocy (bez PoE) nie może być większy niż 35W. |
| Gwarancja | Dożywotnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory), obowiązując tak długo jak produkt jest oferowany przez producenta + 5 lat od momentu zakończenia produkcji.Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |
| Dokumenty | Wykonawca winien przedłożyć dokumenty:1. Deklaracja zgodności CE oferowanego urządzenia – certyfikat potwierdzony za zgodność z oryginałem,
2. Oświadczenie producenta lub oświadczenie autoryzowanego przedstawiciela producenta potwierdzające zgodność wszystkich parametrów oferowanego urządzenia wskazanych w Opisie przedmiotu zamówienia.
 |

# System bezpieczeństwa sieci NGFW (UTM)

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. 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.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

• Firewall.

• Ochrony w warstwie aplikacji.

• Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.

3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

4. Monitoring stanu realizowanych połączeń VPN.

5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

• 18 portami Gigabit Ethernet RJ-45.

• 8 gniazdami SFP 1 Gbps.

• 4 gniazdami SFP+ 10 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.

4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6 Gbps.

4. Wydajność szyfrowania IPSec VPN nie mniej niż 34 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2,5 Gbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

12. Analiza ruchu szyfrowanego protokołem SSH.

13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH).

Polityki, Firewall

14. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

15. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

• Translację jeden do jeden oraz jeden do wielu.

• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

16. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

17. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

18. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

• Amazon Web Services (AWS).

• Microsoft Azure

• Google Cloud Platform (GCP).

• OpenStack.

• VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

• Wsparcie dla IKE v1 oraz v2.

• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

• Obsługa protokołu Diffie-Hellman grup 19 i 20.

• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

• Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

• Routingu statycznego.

• Policy Based Routingu.

• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

4. Uwierzytelnianie w oparciu o protokół SAML.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

• ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

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

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, 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.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Scentralizowany system rejestrowania i analizy logów

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.

2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.

2. Możliwość przeglądania logów historycznych z funkcją filtrowania.

3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.

5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.

6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.

2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.

3. Funkcję definiowania własnych raportów.

4. Możliwość spolszczenia raportów.

5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.

2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

• Malware.

• Aplikacje sieciowe.

• Email.

• IPS.

• Traffic.

• Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

2. Wsparcie: System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. 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.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

• Firewall.

• Ochrony w warstwie aplikacji.

• Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.

3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

4. Monitoring stanu realizowanych połączeń VPN.

5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

• 18 portami Gigabit Ethernet RJ-45.

• 8 gniazdami SFP 1 Gbps.

• 4 gniazdami SFP+ 10 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.

4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B.

3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6 Gbps.

4. Wydajność szyfrowania IPSec VPN nie mniej niż 34 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.

6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2,5 Gbps.

7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

5. Ochrona przed atakami - Intrusion Prevention System.

6. Kontrola stron WWW.

7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

8. Zarządzanie pasmem (QoS, Traffic shaping).

9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

12. Analiza ruchu szyfrowanego protokołem SSH.

13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH).

Polityki, Firewall

14. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

15. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

• Translację jeden do jeden oraz jeden do wielu.

• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

16. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

17. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

18. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

• Amazon Web Services (AWS).

• Microsoft Azure

• Google Cloud Platform (GCP).

• OpenStack.

• VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

• Wsparcie dla IKE v1 oraz v2.

• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

• Obsługa protokołu Diffie-Hellman grup 19 i 20.

• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.

• Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

• Routingu statycznego.

• Policy Based Routingu.

• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

4. Uwierzytelnianie w oparciu o protokół SAML.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

• ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

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

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, 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.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

# Serwer pocztowy raz z systemem ochrony poczty internetowej

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.

2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

Funkcje serwera poczty

W tym zakresie dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.

2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2).

3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.

4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3).

5. Polski interfejs użytkownika przy dostępie przez WebMail.

6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.

7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.

2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.

3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).

4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.

5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).

6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.

7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.

8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.

9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.

10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.

11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.

12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.

13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.

14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.

15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.

16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.

17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.

2. Kwarantannę dla zainfekowanych plików.

3. Skanowanie załączników skompresowanych.

4. Definiowanie komunikatów powiadomień w języku polskim.

5. Blokowanie załączników w oparciu o typ pliku.

6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.

7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.

8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

9. Ochronę typu wirus outbrake.

10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.

2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.

3. Szczegółowa kontrola nagłówka wiadomości.

4. Analiza Heurystyczna.

5. Współpraca z zewnętrznymi serwerami RBL, SURBL.

6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.

7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.

8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.

9. Kontrola w oparciu o Greylisting oraz SPF.

10. Filtrowanie treści wiadomości i załączników.

11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.

12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.

13. Ochrona typu outbrake.

14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).

15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.

16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)

17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).

2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.

3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.

4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).

5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.

2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.

3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.

4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.

5. Możliwość analizy przebiegu sesji SMTP.

6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.

7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.

8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.

2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.

3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.

4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.

2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.

2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.

3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje

System musi być dostarczony w modelu „na własność” tj. Niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

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

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 60 miesięcy.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

# Serwery pod wirtualizację

**3 sztuki**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
* Serwer z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy
* Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
 |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów.
* Obsługa procesorów 64 rdzeniowych.
* Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
* Płyta główna powinna obsługiwać do 8TB pamięci RAM w konfiguracji dwuprocesorowej.
 |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
 |
| **Procesor** | * Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.8GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 336 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
 |
| **RAM** | * Minimum 256GB DDR5 RDIMM 5600MT/s,
* Na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci.
 |
| **Funkcjonalność pamięci RAM** | * Demand Scrubing,
* Patrol Scrubing,
* Permanent Fault Detection
 |
| **Gniazda PCI** | * minimum jeden slot PCIe generacji 5
 |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Interfejsy SFP28 muszą być wyposażone we wkładki 10Gb SFP+ MM.* Dodatkowa, dwuportowa karta 32GB FC wraz z wkładkami MM

4 światłowody LC-LC OM3 3m |
| **Dyski twarde** | * Zainstalowane dwa dyski M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
 |
| **Wbudowane porty** | * 4 x USB z czego nie mniej niż 1x USB 3.0, 1x VGA
 |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
 |
| **Zasilacze** | * Redundantne, Hot-Plug min. 1100W każdy wraz z kablami zasilającymi o długości min. 2m.
 |
| **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 V3
* 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
 |
| **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;
	+ 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
	+ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej

oraz z możliwością rozszerzenia funkcjonalności o:* + Przesyłanie danych telemetrycznych w czasie rzeczywistym
	+ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze
	+ Automatyczna rejestracja certyfikatów (ACE)
 |
| **System operacyjny / dodatkowe oprogramowanie** | Windows Server 2022 Datacenter na odpowiadającą CPU liczbę rdzeni.Licencje Windows Server 2022 User CAL – 80 sztuk per serwer. |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:
	+ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
	+ integracja z Active Directory
	+ 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
	+ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
	+ 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
	+ Integracja z service desk producenta dostarczonej platformy sprzętowej
	+ Możliwość przejęcia zdalnego pulpitu
	+ Możliwość podmontowania wirtualnego napędu
	+ Kreator umożliwiający dostosowanie akcji dla wybranych alertów
	+ Możliwość importu plików MIB
	+ Przesyłanie alertów „as-is” do innych konsol firm trzecich
	+ Możliwość definiowania ról administratorów
	+ 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 automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
	+ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
	+ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
	+ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
	+ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
	+ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
	+ Zdalne uruchamianie diagnostyki serwera.
	+ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
	+ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Licencja na to oprogramowanie nie jest wymagana na tym etapie postępowania. |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001
* Serwer musi posiadać deklaracja CE.
* Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
 |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.
* Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
 |
| **Warunki gwarancji** | 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie lub przez Internet.Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.Zamawiający wraz z ofertą wymaga oświadczenia producenta serwera, że zaoferowany sprzęt pochodzi i oficjalnego kanału sprzedaży producenta, oraz że serwis zaoferowanego sprzętu będzie realizowany przez producenta i/lub we współpracy z autoryzowanym serwisem producenta oraz że, w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej producent przejmie na siebie wszelkie zobowiązania związane z serwisem oferowanego sprzętu. |

# Macierz dyskowa

**1 sztuka**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne pojedynczej macierzy** |
| Obudowa | Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu. |
| Kontrolery dyskowe | Minimum dwa kontrolery pracujące w trybie Symmetrical Active-Active (SAN-only), to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery muszą pozwalać na udostępnianie zasobów protokołem FC, iSCSI w zależności od zastosowanych kart komunikacyjnych. Komunikacja pomiędzy parą kontrolerów (synchronizacja cache) macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband.Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze wielu kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego.Kontrolery muszą być wyposażone w procesory o sumarycznej ilości min. 48 rdzeni (ang.: core) |
| Możliwość rozbudowy  | Macierz umożliwia rozbudowę do 6 par kontrolerów dyskowych tworzących jedna logiczną macierz, bez konieczności wymiany zaoferowanej pary kontrolerów.Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązanie oparte o wirtualizator.Macierz musi umożliwiać rozbudowę do co najmniej 70 sztuk oferowanego typu modułów pamięci, bez wymiany kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek i modułów NVMe oraz przełączników, jeśli rozbudowa o dużą liczbę półek tego wymaga). Półki dyskowe muszą być podłączane poprzez porty o przepustowości min. 50Gb/s z obsługą protokołu RDMA. |
| Wymagana przestrzeń | Macierz musi być skonstruowana wyłącznie do obsługi modułów pamięci NVMe i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych.Moduły pamięci NVMe muszą być wyposażone w podwójne, redundantne interfejsy PCIe. Min 20 dysków NVMe o pojemności 3.84TB.Nie dopuszcza się dysków opartych o komórki QLC |
| Pamięć Cache | Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 192 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin. |
| Zabezpieczenie danych | Urządzenie musi obsługiwać poziomy RAID5 i RAID6 (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare) lub równoważne poziomy RAID zabezpieczające przed awarią dwóch dysków jednocześnie.Macierz musi umożliwiać również skonfigurowanie poziomu RAID zapewniającego odporność na jednoczesną awarię 3 dysków.Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. |
| Dostępne interfejsy | Każdy kontroler udostępnia minimum:Porty front-end:* 4 interfejsy 10Gb Eth SFP+
* 4 interfejsy 32Gb FC obsługujących protokół NVMe over FC

Macierz umożliwia rozbudowę każdego kontrolera o dodatkowe interfejsy minimum:4 porty FC 32Gb/s obsługujących protokół NVMe over Fibre Channel w ramach zaoferowanej ilości kontrolerów oraz możliwość podłączania serwerów bezpośrednio do tych portów macierzy bez użycia przełączników. Wszystkie porty muszą być obsadzone odpowiednimi modułami SFP+/SFP28.Macierz musi być wyposażone w komplet okablowania w tym kable zasilające. |
| Brak pojedynczego punktu awarii | Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy. |
| Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (Thin Provisioning) | Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| Snapshoty | Urządzenie musi umożliwiać utworzenie 800 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 5000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii). |
| Funkcje kopiujące | Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| Redukcja danych | Macierz musi mieć możliwość włączenia funkcjonalności deduplikacji i kompresji danych w trybie in-line, a ponadto musi ona umożliwiać:* włączenie deduplikacji dla poszczególnych wolumenów,
* wyłączenie deduplikacji dla poszczególnych wolumenów na których wcześniej deduplikacja była włączona,
* włączenie kompresji dla poszczególnych wolumenów,
* wyłączenie kompresji dla poszczególnych wolumenów na których wcześniej kompresja była włączona,
* uruchomienia jednocześnie deduplikacji i kompresji dla dowolnego wolumenu,

Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| Replikacja danych | Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC lub iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| Klaster wysokiej dostępności | Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności” tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych” należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności”, musi wspierać klastrowanie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności” musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności” musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| Priorytety zadań | Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| Wielościeżkowość | Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows Server 2016/2019, Vmware 7.X i 8.X, CentOS. |
| Zasilanie  | Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap. |
| Zarządzanie macierzą | Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów NVME. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI co najmniej 1 rok wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożlwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| Serwisowalność | Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii.Zgłoszenia usterek muszą być akceptowane zarówno drogą email jak również drogą telefoniczną. |
| Gwarancja, wsparcie serwisowe | Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.Macierz dyskowa musi zostać objęta minimum 5 letnim okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.Moduły NVMe mają być objęte gwarancją, która po awarii modułu nie wymaga zwrotu wymienionego dysku do producenta lub partnera serwisowego - niesprawny dysk pozostaje u Zamawiającego.Usługi gwarancyjne świadczone przez wykonawcę/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001:2008 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001:2008 lub równoważny.Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:* bezpłatna możliwość aktualizacje firmware;
* dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń;
* dostęp do centrum pomocy technicznej producenta;
* otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware;
* otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy
 |

# Serwer backup

**1 sztuka**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3,5" Hot-Plug oraz 2 dysków 2,5” Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych |
| **Procesor** | Zainstalowany jeden procesor, min. 16-rdzeniowy, min. 3.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 177 w teście SPECrate2017\_int\_base w konfiguracji jedno procesorowej, dostępnym na stronie [www.spec.org](http://www.spec.org).Możliwość obsługi procesorów 128 rdzeniowych |
| **RAM** | Minimum 64GB DDR5 RDIMM 4800MT/s, na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do min. 3TB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Patrol Scrubbing lub inne |
| **Gniazda PCI** | Minimum 6 slotów PCIe, z czego przynajmniej 2 x16 |
| **Interfejsy sieciowe/FC/SAS** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)Interfejsy SFP28 muszą być wyposażone we wkładki 10Gb SFP+ MM.Dodatkowa, dwuportowa karta 32GB FC wraz z wkładkami MM. |
| **Dyski twarde** | Zainstalowane: * 12 dysków SAS o pojemności min. 16TB, 12Gbps, Hot-Plug.
* 2 dyski SSD vSAS RI o pojemności min. 960GB 12Gbps, Hot-Plug.

Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60 |
| **Wbudowane porty** | 3x USB w tym przynajmniej 1x USB 3.01x port VGA na przednim panelu obudowyMożliwość rozbudowy o port RS232 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1080 |
| **System operacyjny / dodatkowe oprogramowanie** | Windows Server 2022 Standard na odpowiadającą CPU liczbę rdzeni. |
| **Wentylatory** | Redundantne |
| **Zasilacze** | Redundantne, Hot-Plug min. 1100W każdy wraz z kablami zasilającymi o długości min. 2m. |
| **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
 |
| **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 (np. 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;
* 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
 |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:
	+ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
	+ integracja z Active Directory
	+ 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
	+ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
	+ 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
	+ Integracja z service desk producenta dostarczonej platformy sprzętowej
	+ Możliwość przejęcia zdalnego pulpitu
	+ Możliwość podmontowania wirtualnego napędu
	+ Kreator umożliwiający dostosowanie akcji dla wybranych alertów
	+ Możliwość importu plików MIB
	+ Przesyłanie alertów „as-is” do innych konsol firm trzecich
	+ Możliwość definiowania ról administratorów
	+ 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 automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
	+ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
	+ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
	+ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
	+ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
	+ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
	+ Zdalne uruchamianie diagnostyki serwera.
	+ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
	+ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Licencja na to oprogramowanie nie jest wymagana na tym etapie postępowania. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001Serwer musi posiadać deklarację CE.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | 5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie lub przez Internet.Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.Zamawiający wraz z ofertą wymaga oświadczenia producenta serwera, że zaoferowany sprzęt pochodzi i oficjalnego kanału sprzedaży producenta, oraz że serwis zaoferowanego sprzętu będzie realizowany przez producenta i/lub we współpracy z autoryzowanym serwisem producenta oraz że, w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej producent przejmie na siebie wszelkie zobowiązania związane z serwisem oferowanego sprzętu. |

# Biblioteka taśmowa

**1 sztuka**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa**  | Do zamontowania w szafie rack, maksymalnie 3U, wbudowany czytnik kodów kreskowych, redundantne zasilanie wraz z kablami zasilającymi. |
| **Napęd** | 1x LTO8 z możliwością rozbudowy biblioteki taśmowej do min. 20 napędów LTO. |
| **Interfejs** | FC |
| **Liczba slotów** | 40 w tym minimum pięć slotów we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotówW komplecie min.:* 1 taśma czyszcząca
* 40 taśm LTO8
* Etykiety do taśm LT08 o numerach 1-200
 |
| **Dodatkowe** | * interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD
* wyjmowane magazynki kieszeni na taśmy w celu łatwego zarządzania większą ilością taśm
* wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja)
* Obsługa SNMP, TLS1.2 oraz IP6
* Wsparcie dla technologii szyfrowania backupowanych danych.
 |
| **Gwarancja** | Pięć lat gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. * 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).
* Wymagana instalacja urządzenia w szafie serwerowej rack.
* Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty.
* Zamawiający wraz z ofertą wymaga oświadczenia producenta serwera, że zaoferowany sprzęt pochodzi i oficjalnego kanału sprzedaży producenta, oraz że serwis zaoferowanego sprzętu będzie realizowany przez producenta i/lub we współpracy z autoryzowanym serwisem producenta oraz że, w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej producent przejmie na siebie wszelkie zobowiązania związane z serwisem oferowanego sprzętu.
 |

# Oprogramowanie do wirtualizacji

**Licencja subskrypcyjna na 5 lat obsługująca 3 serwery, każdy z jednym procesorem szesnasto-rdzeniowym**

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy fizyczny procesor wymaga przypisania do niego licencji w ilości zgodnej z liczbą fizycznych rdzeni, jednak nie mniejszej niż 16 licencji na rdzenie.
4. Licencja na konsolę do zarządzania środowiskiem wirtualnym musi być zawarta w licencji na oferowany wirtualizator. Ilość licencji na konsolę zarządzającą do rozwiązania determinuje sumaryczna ilość posiadanych licencji na rdzenie fizycznych procesorów.
5. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
11. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
12. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
13. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10/11, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.
14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
15. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
16. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
17. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
18. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
19. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
20. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
21. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności Microsoft Active Directory, Open LDAP.
22. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
23. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
24. Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
25. Rozwiązanie musi zawierać możliwość zabezpieczania maszyn wirtualnych przez rozwiązania antywirusowe firm trzecich bez konieczności instalacji agenta wewnątrz maszyny wirtualnej.
26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
27. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, pomiędzy zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej,
28. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy, bez jakiegokolwiek przestoju i bez utraty danych, jednocześnie między serwerami fizycznymi oraz zasobami dyskowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej.
29. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
30. Rozwiązanie musi zapewniać wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania wszystkich funkcjonalności w tym Hyper-V systemu Windows Server na maszynie wirtualnej.
31. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
32. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.

# Oprogramowanie do backupu

**Jeżeli oprogramowanie licencjonowane jest w formie wieczystej i subskrypcyjnej to Zamawiający wymaga wersji wieczystej pozwalającej na backup 30 maszyn wirtualnych ze wsparciem na 5 lat.**

Wymagane funkcjonalności:

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x i 8.0 oraz Microsoft Hyper-V 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.

Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.

Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.

Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.

Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).

Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.

Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.

Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.

Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.

Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.

Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA)
w celu dostępu do konsoli administracyjnej.

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

Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.

Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.

Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).

Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn
z wykorzystaniem wbudowanej akceleracji WAN.

Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.

Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.

Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).

Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.

Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.

Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.

Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem

Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

# Wdrożenie wszystkich powyższych punktów

###

**Wdrożenie serwerów, macierzy, środowiska wirtualnego i systemu backupu**

Montaż dostarczonego sprzętu w miejscu wskazanym przez Zamawiającego. Podłączenie do zasilania, sieci LAN i SAN.

Instalacja i konfiguracja dostarczonego sprzętu w zakresie:

- konfiguracja adresów managment dostarczonego sprzętu

- instalacja i konfiguracja środowiska wirtualizacyjnego w tym: konfiguracja systemów operacyjnych hypervizora, konfiguracja klastra, sieci LAN oraz SAN.

- instalacja i konfiguracja macierzy dyskowej oraz udostępnienie przestrzeni dyskowej do klastra serwerów wirtualizacyjnych

- instalacja i konfiguracja dostarczonego systemu backupu w tym: instalacja systemu operacyjnego, systemu backupu, konfiguracja polityk backupu wykonujących backup.

- instalacja i konfiguracja biblioteki taśmowej, podłączenie do serwera backupu oraz konfiguracja zadań backupu na taśmy

Migracja do 30 maszyn wirtualnych (do 25TB) z obecnego środowiska wirtualnego VMware (ESX 6.5) do nowego klastra wirtualizacyjnego

Przygotowanie dokumentacji technicznej zawierającej adresację, założone konta oraz hasła

Przeprowadzenie prezentacji wdrożonego rozwiązania w wymiarze 4 godzin

**Wymagania dotyczące wdrożenia**

Ze względu na posiadane przez Zamawiającego oprogramowanie do wirtualizacji Vmware vSphere Zamawiający wymaga, aby firma wdrażająca rozwiązanie miała zatrudnionego na umowę o pracę minimum jednego inżyniera posiadającego certyfikat techniczny VMware vSphere na poziomie minimum VCP

Zamawiający wymaga, aby firma wdrażająca rozwiązanie miała zatrudnionego na umowę o pracę minimum jednego inżyniera posiadającego certyfikat techniczny wydany przez producenta oprogramowania do backupu

Zamawiający wymaga, aby firma wdrażająca rozwiązanie miała zatrudnionego na umowę o pracę minimum jednego inżyniera posiadającego certyfikat techniczny wydany przez producenta macierzy dyskowej.

**Przełączniki**

Dostawa sprzętu

Instalacja w ustalonym z zamawiającym miejscu

- Połączenie z istniejącymi elementami infrastruktury

- Stworzenie stosu przełączników

- Konfiguracja uzgodnionej funkcjonalności L2 (VLANy, agregacjie, UDLD/DLDP, STP)

- Konfiguracja uzgodnionej funkcjonalności L3 (adresy, bramy, DNSy, NTP, syslog)

- Konfiguracja uzgodnionych funkcjonalności bezpieczeństwa

- instalacja oraz uruchomienie systemu do zarządzania przełącznikami (system musi pochodzić od tego samego producenta co oferowane przełączniki)

- podłączenie przełączników do systemu zarządzania przełącznikami

- wykonanie dokumentacji powykonawczej

**System bezpieczeństwa sieci NAC**

Wdrożenie systemu w środowisku witalizacyjnym Zamawiającego

- Aktualizacja systemu do najnowszej wersji

- Wykonanie konfiguracji wstępnej systemu (ustawienie haseł dostępowych, konfiguracja ntp oraz snmp)

- Autentykacja użytkowników za pomocą 802.1x z wykorzystaniem użytkownika i hasła

- Autentykacja urządzenia za pomocą adresu MAC z profilowaniem (DHCP profiling)

- Logowanie gości za pomocą Catpive-Portalu Sieci WiFi

- Logowanie za pomocą TACACS+ do urządzeń sieciowych (dostarczonych w ramach projektu)

**Kolektor i analizator logów**

System zbierania logów:

 Dostawa oprogramowania

 Instalacja oprogramowania w środowisku zamawiającego

 - Konfiguracja warstwy sieciowej

 - Konfiguracja ustawień systemowych

 - Podłączenie urządzeń które mają przesyłać logi do systemu

**System zabezpieczenie sieci NGFW**

Firewall/UTM:

Dostawa sprzętu

Konfiguracja dostarczonego sprzętu i oprogramowania:

-stworzenie klastra urządzeń UTM

-aktualizacja do najnowszej zalecanej wersji oprogramowania

-stworzenie segmentów sieci (VLANów)

-stworzenie przykładowych polityk zezwalających na ruch pomiędzy segmentami

-stworzenie profili bezpieczeństwa

-przełączenie sieci na firewall/UTM

**System ochrony poczty internetowej**

Opis systemu ochrony poczty :

• Pobranie software i instalacja obrazu na maszynie wirtualnej w środowisku VMWare

• konfiguracja interfejsów oraz adresacji

• konfiguracja routingu

• konfiguracja czasu

• konfiguracja ustawień głównych takich jak nazwa hosta domena główna

• konfiguracja domeny oraz subdomen

• Wstępna konfiguracja profili Anty Spam

• Wstępna konfiguracja profili Anty Virus

• Wstępna konfiguracja profili zawartości z blokowaniem plików typu exe

• Konfiguracja profili zasobów

• Konfiguracja polityk

• Konfiguracja ograniczenia wielkości plików oraz wielkości wiadomości oraz czarnych i białych list

• Konfiguracja Sandbox w chmurze

• Konfiguracja ochrony linków

• Konfiguracja rozbrajania i rekonstrukcji treści,

• Umówienie daty i godziny przepięcia

• Przegląd konfiguracji przed przepięciem

• Przepięcie ruchu mailowego na nowy system ochrony poczty