Opis przedmiotu zamówienia

I. Zapora sieciowa Next Generation Firewall

1. Zapora sieciowa typu Next Generation Firewall (NGFW)
2. Mechanizm pozwalający na dwustronną analizę ruchu.
3. Minimalna ilość interfejsów:
    a. 10 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.
    b. 2 interfejsy USB dla przyszłych potrzeb i do podłączenia modemu 3G
    c. 1 interfejs konsoli do zarządzania zaporą
    d. 1 slot rozszerzający
4. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa
5. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji
6. Możliwość utworzenia przynajmniej 50 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q
7. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej
8. Minimalna ilość jednocześnie obsługiwanych połączeń: 150 000
9. Możliwość obsłużenia przynajmniej 12 000 nowych połączeń w ciągu 1 sekundy.
10. Przepustowość urządzenia pracującego w trybie stateful firewall: 1.5 Gbps – dla ramki 1518B zgodnie z RFC 2544
11. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 1.1 Gbps
12. Przepustowość urządzenia pracującego jako koncentrator VPN: 1.1 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544
13. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 500 Mbps
14. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 50
15. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 25.
16. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.
17. Wydajnosc urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 200 Mbps.
18. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP
19. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site)
20. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa).
21. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP.
22. Wsparcie dla Dynamicznego DNS tzw. DDNS
23. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.

24. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inpekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).
25. Administrator powinien mieć możliwosc tworzenia róznych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:
    a. wyświetlenie strony blokady (z możliwością tworzenia kilku róznych stron)
    b. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony
    c. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danj kategorii. Używtkonik może wejść na stronę po akceptacji polityki.
26. Administrator powinien mieć możliwosc stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps
27. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.
28. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.
29. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.
30. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN)
31. Kontrola dostępności zestawionych tuneli VPN
32. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.
33. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.
34. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić)
35. Funkcja NAT oparta o reguły bezpieczeństwa.
36. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)
37. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
38. Zintegrowany system skanowania antyspyware
39. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.
40. System IPS musi używać algorytmu szeregowego przetwarzania.

41. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
42. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji
    a. Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.
    b. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimporotwanie sygnatur
    c. Administrator systemu musi mieć możliwosc skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.
43. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
44. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa
45. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi
46. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p
47. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń
48. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minium 3 silników pochądzących od róznych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkch silnikach. Licencja na tą funkcjonalność nie jest przedmiotem przetargu, ale urządzenie powinno zapewniać taką funkcjonalność w celu późniejszej rozbudowy systemu.

Wymagane licencje:

1. Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji oraz zapewnienie wsparcia technicznego 24x7 na okres 2 lat.

II. Oprogramowanie do tworzenia kopii zapasowych

Wymagania ogólne

Oprogramowanie musi umożliwiać tworzenie kopii zapasowej z dwóch serwerów fizycznych, posiadających po 2 procesory fizyczne każdy.

- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
- Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
- Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V

Całkowite koszty posiadania

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

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

- 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 nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia
- Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki" na wirtualnej maszynie
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.
- Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 5.5, 5.6, 8.0, 8.10 i archiwizować również metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD
- 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 wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO

- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- Oprogramowanie musi automatycznie wykrywać i usuwać snapshotysieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
- Oprogramowanie musi wspierać kopiowanie plików na taśmy
- Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server
- Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu.
  Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą.

Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

- 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 posiadać takie same funkcjonalności replikacji dla Hyper-V
- Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
- Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
- Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

Wymagania RTO

Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania

- 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 jaką migrację swoimi mechanizmami
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure.
- Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
  - **Linux**
    - ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs
  - **BSD**
    - UFS, UFS2
  - **Solaris**
    - ZFS, UFS
  - **Mac**
    - HFS, HFS+
  - **Windows**
    - NTFS, FAT, FAT32, ReFS
  - **Novell OES**
    - NSS
- 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, grupy oraz pozwalać na odtworzenie haseł.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze.
- Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
- Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
- Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
- Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Monitoring

- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 4.1, 5.x oraz 6.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2 oraz 2016 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
- System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez VMware
- System musi mieć możliwość instalacji na systemach operacyjnych w wersjach 64 bitowych:
    - Microsoft Windows 2008 SP2
    - Microsoft Windows 2008 R2 SP1
    - Microsoft Windows 7 SP1
    - Microsoft Windows 8
    - Microsoft Windows 2012
    - Microsoft Windows 2012 R2
    - Microsoft Windows 8.1
    - Microsoft Windows 10
    - Microsoft Windows 2016
- System musi obsługiwać następujące bazy danych w wersjach 32 i 64 bitowych:
    - Microsoft SQL Server 2008
    - Microsoft SQL Server 2008 R2
    - Microsoft SQL Server 2012 R2
    - Microsoft SQL Server 2014
    - Microsoft SQL Server 2016
- System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter

- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
- System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
- Silnik raportowania powinien być oparty o SQL Server Reporting Services w celu zapewnienia bezpiecznego dostępu do raportów dla wielu użytkowników z uwzględnieniem ról, jakie pełnią w organizacji
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
- System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
- System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
- System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
- System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 5.5, 5.6, 8.0 oraz 8.10

Raportowanie

- System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 4.1, 5.x oraz 6.0, vCenter Server 4.1, 5.x oraz 6.0 jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2i 2016.
- System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
- System musi być certyfikowany przez VMware i posiadać status „VMware Ready"
- System musi instalować się na następujących systemach operacyjnych:
    - Microsoft Windows 2008 SP2
    - Microsoft Windows 2008 R2 SP1
    - Microsoft Windows 7 SP1
    - Microsoft Windows 8
    - Microsoft Windows 2012
    - Microsoft Windows 2012 R2
    - Microsoft Windows 8.1
    - Microsoft Windows 10
    - Microsoft Windows 2016
- System musi wspierać jako silnik bazodanowy następujące bazy danych:
    - Microsoft SQL Server 2008
    - Microsoft SQL Server 2008 R2
    - Microsoft SQL Server 2012
    - Microsoft SQL Server 2014
    - Microsoft SQL Server 2016

- System do prezentacji raportów powinien używać SQL Server Reporting Services w celu jednoczesnego dostępu do raportów wielu użytkowników z określonymi przez administrator systemu uprawnieniami.
- System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
- System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
- System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
- System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
- Minimalny interwał czasowy dla zadań kolekcjonowania i raportowania musi wynosić min 1 godzinę
- System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
- System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
- System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn wirtualnych, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
- System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware □ System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
- System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie