Zał. nr 4 , 8/2023

Opis przedmiotu zamówienia - wymagania minimalne

System do przechowywania kopii bezpieczeństwa oraz urządzeń firewall typu UTM

I. System kopii bezpieczeństwa

System kopii bezpieczeństwa musi składać się z poniższych komponentów o minimalnych wymaganiach opisanych poniżej.

Serwer – funkcją komponentu ma być wykonywanie i przechowywanie kopii bezpieczeństwa oraz testowe odtworzenie wykonanych na nim kopii bezpieczeństwa. Komponent montowany w głównej szafie serwerowej.

1) Obudowa
    a. Typu RACK, wysokość nie więcej niż 2U;
    b. Szyny umożliwiające wysunięcie serwera z szafy stelażowej oraz ramię porządkujące ułożenie przewodów z tyłu serwera;
    c. Możliwość zainstalowania 10 dysków twardych hot plug 3,5”;
    d. Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;
    e. Zainstalowane 2 szt. dysków SSD SATA 480GB
    f. Zainstalowane 6 szt. dysków SATA 6TB
2) Płyta główna
    a. Dwuprocesorowa;
    b. Wyprodukowana i zaprojektowana przez producenta serwera
    c. Zainstalowany moduł TPM 2.0;
    d. 7 złącz PCI Express generacji 4 w tym (minimum 3 złącza aktywne, możliwe do obsadzenia):
        i. 4 fizyczne złącza o prędkości x16;
        ii. 3 fizyczne złącza o prędkości x8;
        iii. Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
        iv. Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e;
    e. 32 gniazda pamięci RAM;
    f. Obsługa minimum 4TB pamięci RAM DDR4;
    g. Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna
    h. Wsparcie dla technologii:
        i. Memory Scrubbing
        ii. SDDC
        iii. ECC
        iv. Memory Mirroring
        v. ADDDC;
    i. Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)
    j. Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;

3) Procesory
    a. Zainstalowany jeden procesor 8-rdzeniowy
    b. architektura x86_64

   osiągający w teście SPEC CPU2017 Integer Rate Results wynik SPECrate2017_int_base minimum 130 pkt (wynik dla konfiguracji dwuprocesorowej). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/cpu2017.html
4) Pamięć RAM
    a. 64 GB pamięci RAM
    b. DDR4 Registered
    c. 3200Mhz
5) Kontrolery LAN
    a. Karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x 1Gbit Base-T, możliwość wymiany zainstalowanych interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
    b. Zainstalowana karta 2x10Gbit SFP+, wraz z modułami SFP+.
6) Kontrolery I/O
    a. Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug;
    b. Zainstalowany kontroler SAS, NVMe, RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 2GB pamięci cache (opcjonalnie możliwość zabezpieczenia za pomocą baterii lub kondensatora)
    c. Zainstalowana dwuportowa karta FC 16Gb wraz z modułami SFP+ 16Gb.
7) Porty
    a. Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
    b. 2 port USB 3.0 wewnętrzne;
    c. 2 porty USB 3.0 dostępne z tyłu serwera;
    d. 2 porty USB 3.0 na panelu przednim
    e. Zainstalowany port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
    f. Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;
8) Zasilanie, chłodzenie
    a. Redundantne zasilacze hotplug o mocy minimalnej 900W;
    b. Redundantne wentylatory hotplug;
9) Zarządzanie
    a. Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii. Informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
        i. karty rozszerzeń zainstalowane w dowolnym slocie PCI Express
        ii. procesory CPU
        iii. pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM
        iv. wbudowany na płycie głównej nośnik pamięci M.2 SSD

v. status karty zrządzającej serwera
vi. wentylatory
vii. bateria podtrzymująca ustawienia BIOS płyty główne
viii. zasilacze

10) Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
    a. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
        i. Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
        ii. Dostęp poprzez przeglądarkę Web, SSH;
        iii. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
        iv. Zarządzanie alarmami (zdarzenia poprzez SNMP)
        v. Możliwość przejęcia konsoli tekstowej
        vi. Możliwość zarządzania przez 6 administratorów jednocześnie
        vii. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
        viii. Obsługa serwerów proxy (autentykacja)
        ix. Obsługa VLAN
        x. Możliwość konfiguracji parametru Max. Transmission Unit (MTU)
        xi. Wsparcie dla protokołu SSDP
        xii. Obsługa protokołów TLS 1.2, SSL v3
        xiii. Obsługa protokołu LDAP
        xiv. Synchronizacja czasu poprzez protokół NTP
        xv. Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej
    b. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
    c. Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
    d. Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
    e. Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

11) Wspierane OS
    a. Microsoft Windows Server 2022, 2019, 2016

a. VMWare vSphere 7.0, 8.0
b. Suse Linux Enterprise Server 15
c. Red Hat Enterprise Linux 7.9, 8.3

12) Wraz z serwerem należy dostarczyć licencję na oprogramowanie VMware vSphere Essentials Kit wraz z 3 letnim okresem subskrypcji lub oprogramowanie równoważne. Oprogramowanie musi umożliwiać uruchamianie maszyn wirtualnych działających obecnie na środowisku VMware vSphere w infrastrukturze Zamawiającego.
13) Wraz z serwerem należy dostarczyć licencję na oprogramowanie Windows Server 2022 Standard, pozwalającą na instalację oprogramowania do tworzenia kopii bezpieczeństwa dostarczonego w ramach tego postępowania.
14) Gwarancja
    a. 36 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia roboczego od zgłoszenia. Zgłoszenia serwisowe przyjmowane przez 9 godzin, 5 dni w tygodniu. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
    b. Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
    c. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej;
    d. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
    e. Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
    f. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki;
15) Dokumentacja, inne
    a. Elementy, z których zbudowany jest serwer muszą być produktami producenta serwera lub być przez niego certyfikowane oraz cały musi być objęty gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta;
    b. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – na żądanie Zamawiającego oferent dostarczy oświadczenie wykonawcy lub producenta;
    c. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz adres email, na który można zgłaszać usterki;
    d. W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
    e. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

f. Zgodność z normami: CB, RoHS, WEEE oraz CE;

<u>Oprogramowanie do wykonywania kopii bezpieczeństwa</u> - funkcją komponentu jest zarządzanie, uruchamianie oraz monitorowanie zadań wykonywania kopii bezpieczeństwa

1) Wykonawca musi dostarczyć licencje wieczyste w ilości umożliwiającej jednoczesne wykonanie kopii bezpieczeństwa minimum 10 systemów.
2) Dostarczone oprogramowanie musi być objęte wsparciem producenta na okres 36 miesięcy umożliwiające dostęp do wszelkich poprawek i aktualizacji, które producent wprowadzi w tym okresie.
3) Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
4) 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.
5) Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
6) Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
7) 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
8) 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.
9) 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.
10) Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
11) Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
12) Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
13) 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)

14) Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
15) Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
16) 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
17) Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
18) Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
19) Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
20) Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
21) Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
22) 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 datastor
23) 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.
24) Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
25) Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
26) Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Quantum DXi
27) 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.
28) Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
29) 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.
30) 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.
31) Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
32) Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)

33) Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
34) 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 i Hyper-V.
35) Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
36) 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
37) Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
38) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
39) 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
40) 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.
41) Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, Mac,
42) Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
43) Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
44) 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.
45) 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.
46) 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.
47) 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.

48) 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.
49) 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.
50) Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
51) Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
52) Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
53) 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)
54) Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
55) 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
56) 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.
57) Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
58) Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
59) Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
60) Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
61) Rozwiązanie musi wspierać system operacyjny macOS
62) Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS
63) Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
64) Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster

65) Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
66) Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
67) Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
68) Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
69) Rozwiązanie musi wspierać kontrolę pasma sieciowego
70) Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
71) Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
72) Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
73) Rozwiązanie musi wspierać technologię BitLocker
74) Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
75) Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
76) Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
77) Rozwiązanie musi wspierać szyfrowanie
78) Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
79) Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
80) Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej

Biblioteka taśmowa – funkcją komponentu jest przechowywanie kopii bezpieczeństwa wykonywanych i przechowywanych na serwerze. Komponent montowany w głównej szafie serwerowej.

1) Obudowa typu RACK, wysokość nie więcej niż 1U
2) 8 slotów na taśmy LTO
3) 2 magazynki
4) 1 slot i 1 czytnik kodów kreskowych
5) 1 napęd taśmowy LTO 8 FC
6) 10 taśm LTO 8, 1 taśma czyszcząca

7) 1 zasilacz
8) Interaktywny panel sterowania LCD
9) Zdalne zarzadzanie poprzez osobny interfejs Ethernet RJ 45, Remote Management Interface przez HTTPS, wielojęzyczny
10) Czas inicjalizacji 80-120s
11) Średni czas wymiany nośników 45 s
12) Zasilanie AC 100-240 Volt (50 – 60 Hz)
13) Ilość cykli między awariami 2.000.000
14) Pobór energii 80W
15) Kompatybilność z oprogramowaniem do wykonywania kopii bezpieczeństwa: Veritas BackupExec, Veeam, Acronis.
16) Wymiary: 48,2 x 80,6 x 4,4 cm
17) Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego przez okres 36 miesięcy.
18) Oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski, i mających swoją siedzibę na terenie Polski.
19) Podmiot realizujący serwis powinien posiadać ISO 9001 w zakresie świadczenia usług serwisowych, konieczne przedstawienie właściwego certyfikatu

Deduplikator – funkcją komponentu jest deduplikacja kopii bezpieczeństwa wykonywanych i przechowywanych na serwerze. Komponent montowany w szafie umieszonej w GPD w innej lokalizacji.

1) Dostarczone urządzenie musi posiadać, co najmniej 16 TB powierzchni netto (po odjęciu przestrzeni wykorzystywanej na zabezpieczenie RAID) przeznaczonej na przechowywanie unikalnych segmentów danych (deduplikatów). Urządzenie powinno umożliwiać rozbudowę powierzchni do co najmniej 300 TB netto - powyższa wartość musi być możliwa do rozbudowania w ramach dostarczanego applaince sprzętowego. Niedopuszczalne jest użycie innych narzędzi, bramek czy tierowania do chmury w celu zwiększenia pojemności.
2) Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. Deduplikacja zmiennym blokiem musi być wykonywana dla wszystkich protokołów nieważne jakim interfejsem dostępowym zostały one zapisane.
3) Unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
4) Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej
5) Proces deduplikacji powinien odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia.
6) Oferowane urządzenie musi posiadać minimum:
   a) 1 port 1GbE Copper (miedź),
   b) 2 porty 10GbE Optical (wraz z modułem SFP+)
7) Urządzenie musi posiadać nadmiarowe zasilanie

8) Urządzenie musi posiadać możliwość rozbudowy do minimum 16 dodatkowych portów 10GbE lub 8 portów 16Gb FC lub 8 portów 25 GbE
9) Oferowany produkt musi posiadać wsparcie dla minimum następujących protokołów dostępowych:
   a) CIFS, NFS, OST, RMAN SBT API, VDSM
   b) Deduplikacja na źródle dla systemu plików.
10) Urządzenie musi umożliwiać składowanie danych poprzez udostępnianie minimum 128 zasobów NAS w sieci Ethernet wykorzystując protokoły CIFS, NFS.
11) Wymagane jest dostarczenie licencji, pozwalającej na obsługę protokołów CIFS, NFS, OST, deduplikacji na źródle. Licencje muszą być dostarczone na całe urządzenie i do pełnej pojemności urządzenia.
12) Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych wszystkimi protokołami (CIFS, NFS, OST, VTL, RMAN SBT API, VDMS) przechowywanych w obrębie całego urządzenia. Globalna deduplikacja musi wykorzystywać unikalne dane zapisane różnymi protokołami i różnymi interfejsami.
13) Oferowany produkt musi posiadać obsługę deduplikacji na źródle dla zamontowanych zasobów sieciowych (plikowych).
14) Oferowane urządzenie musi wspierać, co najmniej następujące aplikacje Microfocus Data Protector, Veritas NetBackup, Oracle Secure Backup, Nakivo, CommVault, Veeam.
15) W przypadku współpracy z aplikacją Oracle RMAN, urządzenie musi umożliwiać deduplikację na źródle (deduplikację po stronie media serwera). Deduplikacja taka musi zapewniać by z serwerów do urządzenia były transmitowane tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.
16) Oferowany produkt musi umożliwiać replikację danych realizowaną między urządzeniami. Replikacja powinna umożliwiać szyfrowanie przesyłanych danych - długość klucza minimum 256-bit.
17) Urządzenie musi umożliwiać replikację danych z mniejszymi i z większymi modelami urządzeń tego samego producenta.
18) Replikacja musi być możliwa w trybie co najmniej 2 do 1 (fan-in) oraz co najmniej 1 do 2 (fan-out).
19) Oferowane pojedyncze urządzenie musi osiągać wydajność co najmniej 30TB/h (dane podawane przez producenta, bez deduplikacji na źródle) oraz 90TB/h (dane podawane przez producenta, z deduplikacją na źródle).
20) Urządzenie musi być rozwiązaniem kompletnym. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway z uwagi na brak miarodajnych danych dotyczących ich wydajności oraz dostępności. Zamawiający dopuszcza możliwość rozbudowy urządzenia przez dodanie modułów dyskowych.
21) Dostarczone urządzenie musi stanowić całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt), fabrycznie nowe, pochodzić z oficjalnego kanału sprzedaży w Polsce.
22) Gwarancja i serwis
    a. Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego przez okres 36 miesięcy.
    b. Oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski, i mających swoją siedzibę na terenie Polski.
    c. Podmiot realizujący serwis powinien posiadać ISO 9001 w zakresie świadczenia usług serwisowych.

d. Zgłoszenia serwisowe przyjmowane w trybie 9x5, przez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię dostępną w trybie 8x5 (należy podać numer infolinii).
e. Komunikacja telefoniczna i elektroniczna powinna być realizowana w języku polskim.
f. Serwis powinien zapewnić rozpoczęcie procedury naprawy przez certyfikowanego serwisanta najpóźniej w następnym dniu roboczym od zgłoszenia
g. Oferent powinien przedłożyć przed podpisaniem protokołu odbioru następujące dokumenty:
   • Oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   • Certyfikat ISO 9001 podmiotu serwisującego.

W ramach realizacji przedmiotu zamówienia dostawy systemu kopii bezpieczeństwa Wykonawca jest zobowiązany do dostawy komponentów określonych w niniejszym dokumencie, ich instalacji, konfiguracji oraz uruchomienia w środowisku Zamawiającego. Środowisko w jakim będzie pracował system kopii bezpieczeństwa musi być odizolowana od środowiska produkcyjnego oraz wszystkie jego elementy muszą być ze sobą zintegrowane.

Odbiór systemu kopii bezpieczeństwa

Podstawą odbioru systemu kopii bezpieczeństwa jest skuteczne wykonanie kopii bezpieczeństwa systemów krytycznych, jej przechowanie oraz skuteczne ich odtworzenie w środowisku testowym systemu kopii bezpieczeństwa.

UWAGA: Parametry wymagane (graniczne) stanowią wymagania, których niespełnienie spowoduje odrzucenie oferty.

II. System Firewall (zapora sieciowa)

System Firewall musi się składać z dwóch urządzeń pracujących w klasterze HA. Każde z urządzeń musi spełniać następujące wymagania minimalne:

1) OBSŁUGA SIECI
   a. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
2) ZAPORA KORPORACYJNA (Firewall)
   a. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
   b. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
   c. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
   d. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii

osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, zdefiniowana aplikacja etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

e. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
f. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
g. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
h. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
i. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
j. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
k. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

3) INTRUSION PREVENTION SYSTEM (IPS)
   a. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
   b. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
   c. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
   d. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
   e. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
   f. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
   g. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
   h. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
   i. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
   j. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

4) KSZTAŁTOWANIE PASMA (Traffic Shapping)

a. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
b. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
c. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
d. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

5) OCHRONA ANTYWIRUSOWA
   a. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
   b. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
   c. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
   d. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
6) OCHRONA ANTYSPAM
   a. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
   b. Ochrona antyspam ma działać w oparciu o:
      i. białe/czarne listy,
      ii. DNS RBL,
      iii. Skaner heurystyczny.
   c. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
   d. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
7) WIRTUALNE SIECI PRYWATNE (VPN)
   a. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
   b. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
      i. PPTP VPN,
      ii. IPSec VPN,
      iii. SSL VPN.
   c. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
   d. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
   e. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
   f. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
   g. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
   h. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

8) FILTR DOSTĘPU DO STRON WWW
    a. Urządzenie ma posiadać wbudowany filtr URL.
    b. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
    c. Administrator ma mieć możliwość dodawania własnych kategorii URL.
    d. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
        i. blokowanie dostępu do adresu URL,
        ii. zezwolenie na dostęp do adresu URL,
        iii. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
    e. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
    f. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
    g. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
    h. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
    i. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
    j. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
9) UWIERZYTELNIANIE
    a. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
        i. lokalną bazę użytkowników (wewnętrzny LDAP),
        ii. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
        iii. usługę katalogową Microsoft Active Directory.
    b. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
    c. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
        i. SSL,
        ii. Radius,
        iii. Kerberos.
    d. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
    e. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
    f. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
    g. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
    h. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
10) ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)
    a. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
    b. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

i. równoważenie względem adresu źródłowego,
ii. równoważenie względem połączenia.

c. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
d. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
e. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
f. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
g. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

11) ROUTING (TRASOWANIE)
a. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
b. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
c. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
d. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

12) ADMINISTRACJA URZĄDZENIEM
a. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
b. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
c. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
d. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
e. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
f. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
g. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
h. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
i. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
j. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
k. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

l. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
m. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
n. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
o. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
p. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
q. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
r. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    I. manualnego eksportu do pliku w dowolnym momencie czasu,
    II. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
s. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
t. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

13) RAPORTOWANIE
a. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
b. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
c. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
d. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
e. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
f. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
g. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
h. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
i. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

14) POZOSTAŁE USŁUGI I FUNKCJE
a. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
b. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
c. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).

d. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
e. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
f. Urządzenie ma posiadać usługę DNS Proxy.
g. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
h. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
i. Urządzenie musi mieć zaimplementowane Open API
j. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
k. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

15) GWARANCJA I SERWIS
a. Urządzenie ma być objęte 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
b. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone drogą telefoniczną, e-mail lub przez dedykowany do tego portal.
c. Serwis i wsparcie realizowane przez certyfikowanych inżynierów
d. Bezpłatna dostępność poprawek i aktualizacji Firmware dożywotnio dla oferowanego urządzenia – jeżeli funkcjonalność ta wymaga dodatkowej licencji producenta/opłaty, takowy element musi być uwzględniona w ofercie
e. Możliwość odpłatnego przedłużenia licencji na usługi bezpieczeństwa
f. Wsparcie producenta w języku polskim, min. w trybie 8/5

16) PARAMETRY SPRZĘTOWE
a. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 Gb.
b. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.
c. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16.
d. Liczba portów światłowodowych 10Gbps – min. 2 z możliwością rozszerzenia do 6.
e. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:
f. Moduł z 8 interfejsami miedzianymi 10/100/1000Mbps
g. Moduł z 4 interfejsami miedzianymi 10Gbps
h. Moduł z 8 interfejsami światłowodowymi 1Gbps
i. Moduł z 4 interfejsami światłowodowymi 10Gbps
j. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
k. Urządzenie ma być wyposażone w min. 2 różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.
l. Przepustowość Firewall (1518 bajtów UDP) – minimum 18Gbps.
m. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 10Gbps.
n. Przepustowość filtrowania Antywirusowego – minimum 3Gbps.
o. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 4Gbps.
p. Liczba tuneli VPN IPSec – minimum 1 000.

q. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300.
r. Liczba tuneli typu SSL VPN (tryb portalu) – minimum 300.
s. Obsługa interfejsów 802.11q (VLAN) – minimum 1336.
t. Liczba równoczesnych sesji – minimum 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę.
u. Rozwiązanie ma być dostarczone jako klaster Ha dwóch urządzeń działających co najmniej w trybie Active/Passive.
v. Urządzenie musi być wyposażone w moduł TPM
w. Urządzenie nie ma limitu na liczbę użytkowników.
x. Liczba reguł filtrowania – minimum 32 768.
y. Liczba tras statycznego routingu – minimum 5 120.
z. Liczba tras dynamicznego routingu – minimum 10 000.
aa. Możliwość instalacji w szafie RACK 19", wysokość urządzenia 1U.

17) SZKOLENIE
    a. Wykonawca, wraz ze sprzętem, jest zobowiązany dostarczyć Zamawiającemu Voucher na autoryzowane przez producenta szkolenie techniczne poświęcone oferowanym urządzeniom do ochrony styku sieci firmowej z Internetem.
    b. Zarówno szkolenie jak i materiały w języku polskim
    c. Długość szkolenia: min: 3 dni x 8 h
    d. Szkolenie kończy się egzaminem i wydaniem certyfikatu poświadczającego zdany egzamin.
    e. Zakres szkolenia powinien odpowiadać co najmniej szkoleniom umożliwiającym osiągnięcie poziomu certyfikacji takich jak: NSE4, CSNA, CCNA.

18) ZAKRES WDROŻENIA
    a. Konfiguracja klastra HA
    b. Konfiguracja adresacji oraz tras routingu statycznego
    c. Konfiguracja sieci VLAN oraz polityk routingu pomiędzy sieciami
    d. Konfiguracja usługi firewall
    e. Konfiguracja NAT
    f. IPS – zgodnie z wymaganiami klienta
    g. Konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS
    h. Konfiguracja SSL- VPN
    i. Konfiguracja polityk filtru stron www

W ramach realizacji przedmiotu zamówienia dostawy urządzeń firewall Wykonawca jest zobowiązany do dostawy urządzeń określonych w niniejszym dokumencie oraz ich instalacji, konfiguracji oraz uruchomienia w środowisku Zamawiającego.

Odbiór systemu Firewall

Podstawą odbioru systemu jest uruchomienie i prawidłowe działanie w środowisku Zamawiającego dostarczonych urządzeń w konfiguracji polityk bezpieczeństwa odpowiadającej co najmniej politykom funkcjonującym na posiadanym firewallu Zamawiającego w zakresie routingu, firewalla, NAT, VPN, DHCP, Content Filter, IPS.

UWAGA: Parametry wymagane (graniczne) stanowią wymagania, których niespełnienie spowoduje odrzucenie oferty.

Oświadczam, że oferowany przedmiot zamówienia -
System do przechowywania kopii bezpieczeństwa oraz urządzeń firewall typu UTM :

Nazwa	Ilość	Producent / Model	Rok produkcji
Serwer	1		
Oprogramowanie do wykonywania kopii bezpieczeństwa	1		
Biblioteka taśmowa	1		
Deduplikator	1		
Urządzenie UTM	2		

spełnia wszystkie przedstawione powyżej parametry i wymagania minimalne .

.....
(imię i nazwisko) uprawnionego przedstawiciela Wykonawcy