ZP.271.25.2024

Załącznik nr 1 do SWZ

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest: **Dostawa sprzętu i oprogramowania wraz z usługą wdrożenia w ramach projektu „Miasto Augustów-Cyberbezpieczny Samorząd" w postępowaniu prowadzonym przez Miasto Augustów**

1. Zamawiający zamierza zakupić oraz uruchomić / wdrożyć sprzęt i oprogramowania, w ilościach wskazanych poniżej:

L.p.	Nazwa	Ilość
1	Urządzenie zabezpieczające sieć klasy UTM	2
2	Oprogramowanie kompleksowo zabezpieczające pocztę elektroniczną email secure gateway	1
3	Oprogramowanie do centralnego zapisywania logów i raportowania ruchu sieciowego oraz automatyzacji procesów	1
4	Aplikacja generująca jednorazowe hasło dla urządzenia mobilnego 20 szt. i urządzenie generujące jednorazowe hasło 10 szt. kpl do autoryzacji dwuskładnikowej	1
5	Dyski twarde do macierzy dyskowej 6 pak	1
6	System operacyjny Windows Server 2022 lub równoważny standard 16 core license pack	5
7	Licencje dostępowe do Windows Server lub równoważny 2022 1 user cal	50
8	Zasilacz centralny UPS 30kVA	1
9	Serwer do wykonywania kopii zapasowych	1
10	Biblioteka taśmowa LTO	1
11	Serwer plikowy NAS	1
12	Oprogramowanie do wykonywania kopii zapasowych	1
13	Serwer produkcyjny	2
14	Zasilacz awaryjny serwerowy UPS	2
15	Przełącznik sieciowy zarządzalny 24 porty (CORE 10G)	1
16	MOPS Wdrożenie domeny Microsoft AD lub równoważny	1
17	MOPS Oprogramowanie do zarządzania tożsamością i dostępem - system operacyjny Windows Server lub równoważny 2022 Standard 16 Core License Pack	2
18	MOPS Zasilacz awaryjny stanowiskowy UPS	8
19	MOPS Przełącznik sieciowy zarządzalny 24 porty	3
20	MOPS Przełącznik sieciowy zarządzalny 48 portów	1
21	Szkolenie specjalistyczne z obsługi UTMa	3

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

2. Szczegółowy opis poszczególnych urządzeń i usług znajduje się w załącznikach ponumerowanych zgodnie z liczbą porządkową.

3.Dostarczony sprzęt musi być fabrycznie nowy, wolny od wszelkich wad i uszkodzeń. Dostarczony sprzęt musi być sprawny, wolny od wad fizycznych i prawnych. Wykonawca dostarczy przedmiot zamówienia dopuszczony do obrotu i stosowania w krajach UE.

4. Wykonawca zobowiązuje się do prawidłowego wykonania przedmiotu zamówienia, zgodnie z wymaganiami określonymi w SWZ, opisie przedmiotu zamówienia i postanowieniami projektu umowy oraz zasadami wiedzy technicznej, zasadami należytej staranności oraz obowiązującymi normami i przepisami.

5. Dla wyspecyfikowanych urządzeń w opisie przedmiotu zamówienia, podane parametry są wartościami minimalnymi, każdy sprzęt o parametrach lepszych, wyższych od wyspecyfikowanych spełnia wymagania określone przez Zamawiającego.

6. Zakres wdrożenia:

- UTM
  1. Dostawa sprzętu.
  2. Stworzenie klastra HA urządzeń UTM.
  3. Aktualizacja do najnowszej zalecanej wersji oprogramowania.
  4. Przeniesienie konfiguracji z dotychczasowych urządzeń.
  5. Dostosowanie konfiguracji do nowych urządzeń.
  6. Weryfikacja poprawności działania polityk zezwalających na ruch pomiędzy segmentami.
  7. Przeniesienie bram na nowy UTM.
  8. Instalacja wszystkich tokenów.
  9. Sprawdzenie poprawności działania VPN z tokenami.
  10. Konfiguracja integracji UTM z AD.

- System zbierania logów
  1. Dostawa oprogramowania.
  2. Instalacja oprogramowania w środowisku zamawiającego.
  3. Zdefiniowanie ADOM i partycjonowanie dysku.
  4. Konfiguracja warstwy sieciowej (L3, routing).
  5. Konfiguracja ustawień systemowych (konta administratorów, SMTP).
  6. Podłączenie urządzeń UTM do odpowiedniego ADOM.
  7. Szkolenie z obsługi.

- Ochrona poczty
  1. Dostawa oprogramowania.
  2. Instalacja oprogramowania w środowisku zamawiającego.
  3. Konfiguracja warstwy sieciowej.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

4. Konfiguracja ustawień systemowych.
5. Konfiguracja profilów bezpieczeństwa.
6. Konfiguracja funkcji Sandbox.
7. Integracja z obecnym systemem pocztowym zamawiającego.
8. Konfiguracja logowania do system zbierania logów.

- Rozbudowa macierzy
  1. Instalacja dysków w posiadanej macierzy.
  2. Aktualizacja firmware macierzy do najnowszej wersji.
  3. Utworzenie nowego LUN na macierzy i wystawienie go dla serwerów VMware.

- Biblioteka taśmowa
  1. Instalacja biblioteki w miejscu wskazanym przez Zamawiającego.
  2. Aktualizacja firmware do najnowszej wersji.
  3. Konfiguracja urządzenia – sieć, dostęp / uprawnienia.
  4. Oklejenie taśm i załadowanie ich do biblioteki taśmowej.

- Urządzenie NAS
  1. Instalacja sprzętu w miejscu wskazanym przez Zamawiającego.
  2. Aktualizacja firmware do najnowszej wersji.
  3. Konfiguracja urządzenia – sieć, dostęp / uprawnienia.
  4. Utworzenie zasobu i wystawienie go do oprogramowania backupowego.

- Serwer backupu – sprzęt i oprogramowanie
  1. Instalacja sprzętu w miejscu wskazanym przez Zamawiającego.
  2. Aktualizacja firmware do najnowszej wersji.
  3. Podłączenie do posiadanej sieci LAN.
  4. Instalacja i konfiguracja systemu operacyjnego.
  5. Instalacja oprogramowania backupowego. Wgranie licencji.
  6. Podpięcie biblioteki taśmowej.
  7. Dodanie zasobu z urządzenia NAS.
  8. Konfiguracja polityk backupowych na bibliotekę i urządzenie NAS.
  9. Utworzenie pierwszych backupów.

- Przełącznik Urząd
  1. Instalacja w ustalonym z zamawiającym miejscu.
  2. Aktualizacja firmware do najnowszej wersji.
  3. Połączenie z istniejącymi elementami infrastruktury.
  4. Konfiguracja uzgodnionej funkcjonalności L2 (VLANy, agregacje, STP).

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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

- Przełączniki MOPS
  1. Instalacja w ustalonym z zamawiającym miejscu.
  2. Aktualizacja firmware do najnowszej wersji.
  3. Połączenie z istniejącymi elementami infrastruktury.
  4. Konfiguracja uzgodnionej funkcjonalności L2 (VLANy, agregacje, STP).
  5. Konfiguracja uzgodnionej funkcjonalności L3 (adresy, bramy, DNSy, NTP, syslog).

- Serwery zbierania logów
  1. Instalacja sprzętu w miejscu wskazanym przez Zamawiającego.
  2. Aktualizacja firmware do najnowszej wersji.
  3. Podłączenie do posiadanej sieci LAN.
  4. Instalacja i konfiguracja systemu operacyjnego.

- Wdrożenie AD w MOPS
  1. Uruchomienie 2 kontrolerów domeny Windows AD.
  2. Założenie kont wszystkich użytkowników w nowej domenie Active Directory (na podstawie spisu dostarczonego w formie pliku excel zawierającego imię, nazwisko, login).
  3. Utworzenie polityki mapującej zasoby serwera plików (jeśli jest uruchomiony).
  4. Podłączenie 3 stanowisk do nowej domeny AD wraz z migracją profilu użytkownika z konta lokalnego do domenowego. Przeprowadzenie pokazu migracji profilu lokalnego do domenowego Active Directory.

7. Wymagania dotyczące wdrożenia:

- firma wdrażająca powinna dysponować inżynierem posiadającym certyfikat techniczny dostarczonego i wdrażanego oprogramowania do zabezpieczania sieci. Certyfikat powinien zostać wydany przez producenta tego oprogramowania,

- firma wdrażająca powinna dysponować inżynierem posiadającym certyfikat techniczny dostarczonego i wdrażanego producenta oprogramowania do backupu. Certyfikat powinien zostać wydany przez producenta tego oprogramowania,

- firma wdrażająca powinna dysponować inżynierem posiadającym certyfikat techniczny z technologii macierzowych producenta rozbudowywanej macierzy. Certyfikat powinien zostać wydany przez producenta macierzy.

8. Miejsca dostawy:

- Urząd Miejski w Augustowie, ul. Młyńska 35, 16-300 Augustów,

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024
- Miejski Ośrodek Pomocy Społecznej w Augustowie, ul. 3 Maja 60, 16-300 Augustów.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

Szczegółowy opis przedmiotu zamówienia.

1. Urządzenie zabezpieczające sieć klasy 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 3 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:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 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 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 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.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

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

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

2. 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.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. 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
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware vCenter (ESXi).

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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

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.

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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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 np. 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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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

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 Firewall 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 lub równoważny dla funkcji Firewall.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

Serwisy i licencje

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

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 24 miesięcy.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 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 przed zawarciem umowy 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 przed zawarciem umowy oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

2. Oprogramowanie kompleksowo zabezpieczające pocztę elektroniczną email secure Gateway

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 systemu

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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.

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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

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 w 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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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:

VBSpam, VB100 rated, Common Criteria NIAP, FIPS 140-3 Certified lub równoważne.

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:

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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 24 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem producenta przez okres 24 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.

3. Oprogramowanie do centralnego zapisywania logów i raportowania ruchu sieciowego oraz automatyzacji procesów

Wymagania Ogólne

W ramach postępowania wymagane 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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

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 musi 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 dostarczyć dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

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

2. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

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.

Gwarancja oraz wsparcie

System musi być objęty serwisem producenta przez okres 24 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

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć przed zawarciem umowy 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 przed zawarciem umowy oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

4. Aplikacja mobilna generująca jednorazowe hasło dla urządzenia mobilnego 20 szt. i urządzenie generujące jednorazowe hasło 10 szt. kpl do autoryzacji dwuskładnikowej

Opis

W ramach postępowania powinny zostać dostarczone co najmniej 22 tokeny programowe działające na aplikacji mobilmej oraz 10 tokenów sprzętowych, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Zarówno aplikacja jak i tokeny muszą współpracować z urządzeniami zabezpieczające sieć klasy UTM dostarczonymi w tym postępowaniu.

5. Dyski twarde do macierzy dyskowej 6 pak

Opis

Zamawiający wymaga dostarczenia 6 dysków 2.4TB SAS 10k SFF do posiadanej macierzy HPE MSA2062, SN: ACV234W1K6.

6. i 7. System operacyjny Windows Server 2022 standard 16 core license pack lub równoważny

Opis

Wymagane minimalne parametry techniczne oznaczające wymogi równoważne dla systemu Windows Server 2022 standard 16 core
Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

operacyjnego oraz uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Wymaga się dostarczenia 5 licencji na 16 rdzeni każda. Jeżeli system operacyjny wymaga licencji dostępowych należy dostarczyć licencję dla 50 użytkowników.	
Serwerowy System Operacyjny (dalej: SSO) posiada następujące, wbudowane cechy.	
1	Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym.
2	Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
3	Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
4	Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7	Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8	Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
9	Wbudowane wsparcie instalacji i pracy na wolumenach, które: • Pozwalają na zmianę rozmiaru w czasie pracy systemu. • Umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów. • Umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów. • Umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10	Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11	Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12	Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13	Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14	Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

15	Graficzny interfejs użytkownika.
16	Zlokalizowane w języku polskim, następujące elementy: • Menu. • Przeglądarka internetowa. • Pomoc. • Komunikaty systemowe.
17	Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
18	Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
19	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
20	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
21	Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: • Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. • Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: - Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. • Zdalna dystrybucja oprogramowania na stacje robocze. • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. • Centrum Certyfikatów (CA, obsługa klucza publicznego i prywatnego) umożliwiające: - Dystrybucję certyfikatów poprzez http, - Konsolidację CA dla wielu lasów domeny. • Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. • Szyfrowanie plików i folderów. • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). • Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. • Serwis udostępniania stron WWW. • Wsparcie dla protokołu IP w wersji 6 (IPv6).

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	• Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla: - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych, - Obsługi 4 KB sektorów dysków, - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra. • Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model). Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
22	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
23	Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
24	Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
25	Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

8. Zasilacz centralny UPS 30kVA

Opis

Projektuje się zasilacz UPS pracujący w topologii on-line VFI-SS-111, wg normy IEC 62040-3 lub równoważnej, o mocy 30kVA/30kW. Rozwiązanie modułowe, podwyższające niezawodność, niwelujące istnienie pojedynczego punktu awarii – UPS składa się z 2 niezależnych modułów o mocy 15kVA/15kW. Każdy moduł będzie posiadał własny, niezależny tor prostownik-falownik oraz układ ładowania baterii. Moduły wymieniane „na gorąco” (hot-swap) – podczas serwisowania jednego z modułów, drugi pozostaje w trybie podwójnej konwersji (online). UPS będzie wyposażony w wewnętrzny, bezprzerwowy bypass elektroniczny (centralny dla całej szafy UPS). Bypass wewnętrzny będzie posiadał zabezpieczenie przed zwrotnym podawaniem energii do sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040). UPS będzie zasilany dwutorowo – przez tor główny (układ prostownik-falownik) oraz tor rezerwowy (bypass elektroniczny). Dodatkowo będzie wyposażony w zewnętrzny tor obejściowy (serwisowy, mechaniczny). Baterie akumulatorów, zapewniające czas podtrzymania 8 minut dla obciążenia 30kW, będą umieszczone wewnątrz zasilacza UPS.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

Dane techniczne zasilacza awaryjnego UPS:

- UPS pochodzący z seryjnej produkcji; Data wyprodukowania nie może być wcześniejsza niż 6 miesięcy przed dostawą urządzenia,
- producent oferowanego urządzenia powinien posiadać certyfikat ISO 9001 lub równoważny w zakresie projektowania, produkcji, sprzedaży i serwisu systemów zasilania gwarantowanego UPS; Przed zawarciem umowy Wykonawca dostarczy certyfikat ISO 9001 wystawiony przez niezależną jednostkę badawczą,
- moc wyjściowa: 30 kVA/30 kW,
- architektura modułowa: moduły mocy 15kVA/15kW,
- budowa modułowa – każdy moduł jest niezależnym źródłem zasilania i zawiera własny układ prostownik-falownik,
- moduły mocy wymieniane „na gorąco" (hot-swap) – podczas serwisowania jednego z modułów, drugi pozostaje w trybie podwójnej konwersji (online),
- czas podtrzymania bateryjnego: 8 minut dla obciążenia mocą czynną 30kW,
- baterie umieszczone wewnątrz zasilacza UPS,
- ilość faz 3/3 – trzy fazy wejściowe i trzy fazy wyjściowe,
- sprawność w trybie on-line: co najmniej 95,8% w zakresie obciążenia 50-100% (co najmniej 98,5% w trybie oszczędzania energii w zakresie obciążenia 50-100%). Do oferty należy załączyć dokument potwierdzający sprawność oferowanej serii UPS wystawiony przez zewnętrzną jednostkę certyfikującą,
- tolerancja napięcia wejściowego prostownika, bez przejścia na pracę z baterii: 187-276 V,
- częstotliwość wejściowa 50 Hz lub 60 Hz z tolerancją 40Hz do 72Hz,
- wahania napięcia wyjściowego: < 1%,
- wahania częstotliwości wyjściowej: ±0,15 Hz,
- cosϕ wyjściowy = 1,
- cosϕ wejściowy dla 100% obciążenia = 0,99,
- zabezpieczenie przed zwrotnym podaniem energii do sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040 lub równoważne) w torze bypassu statycznego UPS,
- zwarciowy prąd bypassu statycznego I_{cc} – 100 kA,
- urządzenie powinno być wyposażone w system nieciągłego ładowania baterii. Przy dostawie należy dołączyć opis sposobu zarządzania pracą baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni, opis powinien być materiałem firmowym producenta,
- urządzenie powinno posiadać tryb oszczędzania energii, zapewniający automatyczne, bezprzerwowe przełączanie w tryb online (w czasie do 2 ms) w przypadku wystąpienia nieprawidłowości w torze bypassu statycznego. Przy dostawie należy załączyć opis technologii oszczędzania energii, opis powinien być materiałem firmowym producenta,
- inteligentny algorytm zarządzania modułami mocy, regulujący poziom obciążenia poszczególnych modułów w celu uzyskania najwyższej sprawności. Do oferty należy załączyć opis technologii zarządzania modułami mocy, opis powinien być materiałem firmowym producenta,

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- wejściowe zniekształcenia THDi < 3%,
- wyjściowe THDu:
  - dla obciążenia liniowego < 1,5%,
  - dla obciążenia nieliniowego < 3,5%,
- Urządzenie musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:
  - gniazdo komunikacji RS-232,
  - gniazdo wyłącznika awaryjnego p.poż.,
- interfejsy komunikacyjne: SNMP – karta sieciowa Gigabit Ethernet, zgodność ze standardem cyberbezpieczeństwa UL 2900-1 oraz IEC 62443-4-2, szyfrowanie TLS 1.2. Do oferty należy załączyć certyfikaty potwierdzające spełnianie wymaganych norm, wystawione przez niezależną jednostkę badawczą,
- gwarancja realizowana przez autoryzowany serwis producenta min. 24 miesiące od daty uruchomienia,

Zakres wdrożenia zasilacza awaryjnego UPS:

- Dostawa kurierska zasilacza UPS,
- Podłączenie przez autoryzowany serwis producenta zasilacza UPS do przygotowanej przez Zamawiającego instalacji elektrycznej,
- Uruchomienie zasilacza UPS przez autoryzowany serwis producenta,
- Szkolenie z obsługi zasilacza UPS,
- Konfiguracja karty sieciowej SNMP,
- Testy poprawności działania.

Czynności przygotowawcze, które wykona Wykonawca przed podłączeniem zasilacza UPS:

- Zabezpieczenie toru wejściowego prostownika UPS: 3 x 63 A,
- Zabezpieczenie toru wejściowego bypassu statycznego UPS: 3 x 63 A,
- Zabezpieczenie toru wejściowego zewnętrznego bypassu serwisowego: 3 x 63 A,
- Kabel wejściowy toru prostownika UPS: 4 x 16 mm^2,
- Kabel wejściowy toru bypassu statycznego UPS: 4 x 16 mm^2,
- Kabel PE UPS: 1 x 16 mm^2,
- Kabel wejściowy toru zewnętrznego bypassu serwisowego: 5 x 16 mm^2,
- Kabel pomiędzy UPS a bypassem serwisowym: 4 x 16 mm^2,
- Na wejściu UPS będą zabezpieczenia 3-polowe z wkładkami bezpiecznikowymi typu gG/gL,
- Kable będą zakończone odpowiednimi końcówkami i będą umożliwiać podłączenie do zacisków zasilacza UPS (przygotowany zapas okablowania co najmniej 1,5 mb w miejscu instalacji zasilacza UPS).

9. Serwer do wykonywania kopii zapasowych

Opis

Element konfiguracji	Wymagania minimalne

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). Serwer wyposażony w zdejmowany panel przedni z możliwością instalacji zamka chroniącego przed nieuprawionym dostępem do dysków oraz czujnika otwarcia obudowy współpracującego z BIOS/UEFI.
Procesor	Jeden procesor ośmiordzeniowy, x86 - 64 bity, pracujący z częstotliwością bazową min. 2.8 GHz i osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 132 punkty, dla testu oferowanego modelu serwera z 2 procesorami. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org Płyta główna wspierająca zastosowanie procesorów od 4 do 40 rdzeni, moc min. 270W i taktowaniu CPU min. 3.6 GHz
Liczba procesorów	1 procesor
Pamięć operacyjna	Min. 64GB RDIMM DDR4 3200 MT/s w modułach pamięci o pojemności min. 32 GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację minimum 8TB.
Sloty rozszerzeń	Min. 3 aktywne gniazda PCI-Express generacji 4, gniazda pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 1 slot x16 (szybkość slotu – bus width).
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania min. 12 dysków LFF typu Hot Swap, SAS/SATA/SSD 3,5”. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Zainstalowane min. 10 szt. dysków 6TB SAS 7.2k 3,5” typu Hot-swap oraz 2szt. dysków 480 GB M.2 NVMe SSDs (RAID1).
Kontroler	Serwer wyposażony w kontroler sprzętowy z max. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SSD/SATA/SAS.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

Interfejsy sieciowe	Minimum 2 wbudowane porty Ethernet 10 Gb SFP+, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. Porty obsadzone wkładkami 10Gb SFP+ MM. Minimum 2 porty 16 Gb FC.
Karta graficzna	Zintegrowana karta graficzna.
Porty	5 x USB 3.0 (w tym 2 porty wewnętrzne) 1x VGA Wewnętrzny slot na kartę micro SD. Możliwość rozbudowy/rekonfiguracji o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug.
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe, • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP, • dostęp do karty zarządzającej poprzez: - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera, dostęp do karty możliwy: - z poziomu przeglądarki webowej (GUI),

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	- z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP), - z poziomu skryptu (XML/Perl), - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface), • wbudowane narzędzia diagnostyczne, • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego, • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie, • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników, • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough), • obsługa zdalnego serwera logowania (remote syslog), • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów, • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera, a także nagrywanie na żądanie, • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności, • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji, • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping), • zdalna aktualizacja oprogramowania (firmware), • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów, - sterowanie zasilaniem (wł/wył), - ograniczenie poboru mocy dla grupy (power capping),

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	- aktualizacja oprogramowania (firmware), - wspólne wirtualne media dla grupy, • możliwość równoczesnej obsługi przez 6 administratorów, • autentykacja dwuskładnikowa (Kerberos), • wsparcie dla Microsoft Active Directory, • obsługa SSL i SSH, • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli, • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API, • wsparcie dla Integrated Remote Console for Windows clients, • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP).
Systemem operacyjnym	Windows Server Standard 2022 lub równoważny z licencją na odpowiednią liczbę rdzeni lub system równoważny funkcjonalnie, tzn. system z interfejsem w języku polskim, w środowisku, którego możliwe jest bezproblemowe uruchamianie dowolnej aplikacji, działającej poprawnie w systemie Windows Server 2022 PL 64-bit oraz 7 jednoczesnych połączeń do pracy zdalnej na serwerze
Praca zdalna	7 jednoczesnych połączeń do pracy zdalnej na serwerze. Jeżeli jest wymagana licencja, to należy dostarczyć odpowiednią ilość licencji.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Zapewnia wsparcie dla: Microsoft Windows Server 2016, 2019, 2022
Wsparcie techniczne	Minimum 36 miesięcy gwarancja producenta w miejscu instalacji. Czas reakcji 2h w standardowe dni robocze w godzinach od 9:00 do 17:00. Przybycie serwisu do miejsca instalacji w ciągu następnego dnia roboczego od zgłoszenia usterki. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. Uszkodzone dyski pozostają u Zamawiającego.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub równoważne. Deklaracja zgodności CE.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

10. Biblioteka taśmowa LTO

Opis

Należy dostarczyć bibliotekę taśmową spełniającą poniższe parametry.

1. Biblioteka musi obsługiwać co najmniej 24 gniazda na kasety.
2. Obudowa: RACK 2U.
3. Biblioteka wyposażona w napęd FC LTO8.
4. Interfejsy: minimum jeden interfejs sieciowy RJ45; minimum jeden interfejs FC do podłączenia do serwera kopii zapasowych.
5. W zestawie minimum 7 taśm LTO-8 + taśma czyszcząca.
6. Minimum 36 miesięcy gwarancja producenta w miejscu instalacji. Czas reakcji 2h w standardowe dni robocze w godzinach od 9:00 do 17:00. Przybycie serwisu do miejsca instalacji w ciągu następnego dnia roboczego od zgłoszenia usterki. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego urządzenia.

11. Serwer plikowy NAS

Opis

Procesor	Jeden 8-rdzeniowy/16-wątkowy procesor AMD Ryzen™ 7 3700X lub równoważny procesor ośmiordzeniowy osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 22200 pkt W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie https://www.cpubenchmark.net/high_end_cpus.html
Obudowa	Rack 2U o wymiarach nie większych niż, 89× 483 × 565 mm (wys. x szer. x gł.); w zestawie szyny wysuwane do instalacji w szafie RACK
Pamięć RAM	32 GB UDIMM DDR5 z opcja rozszerzenia do 192GB RAM
Ilość obsługiwanych dysków	12 dysków 3,5-calowych 3,5/2,5 dyski SATA
Ilość zainstalowanych dysków	8 dysków o min. pojemności 8TB, MTBF 2mil godzin, cache 256MB. Dyski muszą znajdować się na liście zgodności z oferowanym serwerem NAS
Interfejsy sieciowe	2 porty 1Gigabit sieci Ethernet (RJ45) 2 porty 10GbE (SFP+) 2 porty 10GbE (10GBase-T)
Porty	2 gniazda typu A USB 3.2 Gen 2 10 Gb/s
Porty PCIe	3 gniazda PCIe Gen4
Wskaźniki LED	Dyski, stan, LAN, stan portów rozszerzenia pamięci masowej

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Obsługa RAID	RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity
Funkcje RAID	Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD.
Szyfrowanie	256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych.
System Operacyjny	Apple Mac OS 10.10 lub nowszy Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux IBM AIX 7, Solaris 10 lub nowszy UNIX Microsoft Windows 7, 8, 10 Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019
Stacja monitoringu	Tak, w standardzie 8 darmowych licencji na podłączenie kamer.
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, FC, Telnet, SSH, SNMP
Usługi	Stacja monitoringu Windows ACL Integracja z Windows ADS Serwer WWW Serwer plików Manager plików przez WWW Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI Replikacja w czasie rzeczywistym Serwer RADIUS Klient LDAP Serwer Syslog Container Station
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów.
Język GUI	Polski
Gwarancja i serwis	36 miesięcy gwarancji producenta na NAS 60 miesięcy gwarancji na dyski
Waga	Nie więcej niż 14 kg (netto)
System plików	Dyski wewnętrzne ZFS, EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Funkcje ZFS	Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Ilość połączeń (CIFS)	5000
Liczba migawek	65536
Zasilanie	Redundantne 550 W (x2), 200–240 V
Wentylatory	3 x 60mm, 12VDC
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS

12. Oprogramowanie do wykonywania kopii zapasowych

Opis

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x i 8.x 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.

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 do 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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze 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 tabel, 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.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024
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.

Licencja wieczysta na 30 maszyn wirtualnych. Wsparcie 24 miesiące.

13. Serwer produkcyjny

Opis

Element konfiguracji	**Wymagania minimalne**
Obudowa	Maksymalnie 2U RACK 19 cali wraz z szynami montażowymi.
Procesor	Minimum jeden procesor, min. 12 rdzeni z nominalną częstotliwością pracy min. 2.4 GHz, x86 - 64 bity, osiągające w testach PasMark Average CPU Mark wynik nie gorszy niż 34122 punktów. Wynik testu musi być opublikowany na stronie http://cpubenchmark.net w dniu złożenia oferty.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	Płyta główna wspierająca zastosowanie procesorów od 8 do 48 rdzeniowych, mocy min. 350W.
Liczba procesorów	1 procesor
Pamięć operacyjna	64GB RDIMM DDR5 5600 MT/s w modułach o pojemności 32GB każdy. Płyta główna z minimum 24 slotami na pamięć, umożliwiająca instalację do minimum 4TB. Obsługa zabezpieczeń: Advanced ECC z multi-bit error protection, Online spare
Sloty rozszerzeń	Minimum 6 x PCI-Express 5.0 slots x16. pełnej wysokości. Serwer wyposażony w min. 2 sloty OCP.
Dysk twardy	Miejsca na 24 dyski 3,5" Hot-plug. Zamontowanych min. 12 dysków Hot-plug 16TB SAS 7.2k 3,5". Zainstalowany moduł z dwoma dyskami NVMe M.2 SSD zapewniających minimalną pojemność 480 GB (każdy) i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera i nie zajmować wymaganych slotów PCIe opisanych w sekcji „Sloty roszerzeń”.
Pamięci flash	Serwer umożliwiający instalację pamięci flash w postaci kart microSD zapewniających minimalną pojemność 32 GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera.
Kontroler	Sprzętowy kontroler RAID PCI-e obsługujący 32 porty SAS 12Gb, każdy z min. 8GB pamięcią cache. Obsługiwane poziomy RAID 0,1,10,5,50,6,60.Wsparcie dla dysków SAS / SATA / NVMe
Interfejsy sieciowe	Serwer wyposażony w: - kartę Ethernet 10/25Gb 2-port SFP+ z wkładkami 10Gb SR, - kartę Ethernet 1Gb Base-T 4-port. Powyższe porty nie mogą być osiągnięte poprzez ww. sloty rozszerzeń.
Karta graficzna	Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1920 x 1200 pikseli.
Porty	4 porty USB 3.0 w tym jeden wewnętrzny. 1x VGA

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	Dodatkowy port USB z przodu obudowy umożliwiający serwisowanie i zarzadzanie serwerem. Możliwość rozbudowy o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się stosowania kart PCI.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1800W Titanium.
Bezpieczeństwo	Możliwość doposażania serwera w przedni panel z kluczykiem zabezpieczający dyski przed przypadkowym ich usunięciem.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	• obsługa mechanizmu remote support - automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail • uwierzytelnianie oprogramowania sprzętowego PCIe z protokołem bezpieczeństwa i modelem danych (SPDM) zapewnia integralność komponentu • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power capping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019, 2022 Red Hat Enterprise Linux (RHEL) 9.0 SUSE Linux Enterprise Server (SLES) 15 SP4 VMware ESXi 7.0U3, 8.0 Conconical Ubuntu 22.04 W każdym z zaoferowanych serwerów należy dostarczyć licencję Windows Server 2022 lub równoważną PL 64-bit Standard zgodnie z oferowaną liczbą rdzeni lub system równoważny funkcjonalnie, tzn. system z interfejsem w języku polskim, w środowisku, którego możliwe jest bezproblemowe uruchamianie dowolnej aplikacji, działającej poprawnie w systemie Windows Server 2022 PL 64-bit.
Gwarancja i wsparcie techniczne	Minimum 36 miesięcy gwarancja producenta w miejscu instalacji. Czas reakcji 2h w standardowe dni robocze w godzinach od 9:00 do 17:00. Przybycie serwisu do miejsca instalacji w ciągu następnego dnia roboczego od zgłoszenia usterki. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. Uszkodzone dyski pozostają u Zamawiającego.
Certyfikaty i standardy	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub równoważnymi.

14. Zasilacz awaryjny UPS z dodatkowym modułem bateryjnym

Opis

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań (minimalnych)
1	Moc pozorna	3000 VA
2	Moc rzeczywista	3000 W
3	Współczynnik mocy	1
4	Topologia (klasyfikacja IEC 62040-3)	Line-interactive (czysta sinusoida, AVR)
5	Typ obudowy UPS	Uniwersalna Tower/Rack maks. 2U
6	Liczba, typ gniazd wyjściowych, możliwość sterowania	8x IEC C13 (10A), 2x IEC C19 (16A),

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

		W tym 2 grupy gniazd z możliwością sterowania: 1. 2x IEC C13 2. 2x IEC C13 + 1x IEC C19
7	Typ gniazda wejściowego	Gniazdo IEC C20 (16A)
8	Czas podtrzymania	• 20 minut dla obciążenia 3000W, • 40 minut dla obciążenia 1500W, • możliwość wydłużenia czasu podtrzymania do 75 minut dla obciążenia 3000W poprzez dołożenie kolejnych modułów bateryjnych
9	Napięcie znamionowe	230 V
10	Tolerancja napięcia prostownika	160 - 294 V
11	Częstotliwość znamionowa	50/60 Hz autodetekcja
12	Tolerancja częstotliwości	47 - 70 Hz (system 50 Hz)
13	Napięcie znamionowe wyjściowe	230 V (domyślnie) / 208/220/240 V
14	Częstotliwość wyjściowa	50/60 Hz
15	Baterie wymieniane przez użytkownika "na gorąco"	Tak
16	Ochrona przed przeładowaniem	Tak
17	Ochrona przed głębokim rozładowaniem	Tak
18	Okresowy automatyczny test baterii	Tak
19	Zimny start	Tak
20	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
21	Interfejs komunikacyjny	• USB i RS232
		• karta Web/SNMP
		• złącze dla zdalnego awaryjnego wyłączenia
		• złącze dla zdalnego załączenia/wyłączenia
		• złącze dla wyjściowego styku przekaźnikowego
22	Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS-a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh)
		• Poziomy rząd przycisków sterowania
		• Poziomy rząd wskaźników stanu: trybu normalnego (zielony), trybu bateryjnego (żółty), usterki (czerwony)
		• Pasek LED sygnalizujący stan pracy

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

		• Sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie)
23	Przyciski sterujące	• przycisk Escape (anulowanie)
		• przyciski funkcyjne (przewijanie w górę i w dół)
		• przycisk Enter (potwierdzający)
24	Wyposażenie	• instrukcja obsługi, instrukcja bezpieczeństwa
		• przewód zasilający
		• kabel RS232
		• kabel USB
		• uchwyty kablowe
		• podstawki do montażu pionowego (Tower)
		• 2 przewody IEC 10 A
		• zestaw szyn montażowych do szafy 19"
25	Karta Web/SNMP	• Protokoły i certyfikaty cyberbezpieczeństwa: UL 2900-1/IEC 62443-4-2/HTTPS/MQTTS/ /RADIUS/LDAP/SSH/ pakiet szyfrów TLS 1.2 z minimum SHA256
		• certyfikaty CA i PKI lub równoważne
		• prędkość Gigabit Ethernet
		• różne poziomy nadawania dostępu do konta administratora lub użytkownika
26	Oprogramowanie zarządzające	Oprogramowanie do zarządzania UPS-a w podstawowej funkcjonalności dostarczone wraz z UPS-em. Możliwość dokupienia oprogramowanie producenta UPS-a do monitorowania i zarządzania, umożliwiającego: - tworzenie scenariuszy zasilania ukierunkowanych na pojedyncze maszyny wirtualne, grupy maszyn wirtualnych lub automatyczne grupy maszyn wirtualnych - tworzenie scenariuszy zasilania ukierunkowanych na klastry, w tym w środowiskach hiperkonwergentnych - tworzenie scenariuszy zasilania z sekwencyjnym wyłączaniem poszczególnych maszyn wirtualnych
27	Wyposażenie dodatkowe	Zestaw gniazd wyjściowych PDU o prądzie nominalnym 16A podłączany do gniazda wyjściowego IEC C19 w zasilaczu awaryjnym UPS, obudowa 1U do montażu w szafie Rack (19”) z możliwością montażu w wielu położeniach, z 12 szt. gniazd IEC C13 (10A) i 1 szt. IEC C19 (16A), z 2 bezpiecznikami nadmiarowoprądowymi, z zaciskami zabezpieczającymi przed przypadkowym wyciagnięciem kabla zasilającego na gnieździe wejściowym i gniazdach wyjściowych IEC C13.
28	Maks. wymiary UPS (szer. x gł. x wys. w mm)	438 x 603 x 86

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

29	Maks. wymiary modułu bateryjnego 2U (szer. x gł. x wys. w mm)	438 x 603 x 86
30	Poziom hałasu (przy standardowym obciążeniu)	< 40 dB
31	Zgodność z normami UE	Deklaracja zgodności CE
32	Dodatkowe certyfikaty	Raport CB (TUV), ISO 9001 lub równoważne dla producenta urządzenia
33	Gwarancja	Gwarancja producenta min. 36 miesięcy

15. Przełącznik sieciowy zarządzalny 24 porty (CORE 10G)

Opis

L.p.	Minimalne wymaganie dotyczące przełącznika CORE 10G.
	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
1.	Wymagane parametry fizyczne: a) możliwość montażu w stelażu/szafie 19”, b) wysokość maksymalna 1U, c) dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Urządzenie musi zostać dostarczone z 2 zasilaczami umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap), d) zakres temperatur pracy ciągłej co najmniej od -5 do +45 °C, e) zakres wilgotności pracy co najmniej 10% - 95%, f) port USB.
2.	Przepływ powietrza przód-tył (od strony portów w kierunku zasilaczy).
3.	Urządzenie musi być wyposażone w redundantne wentylatory z możliwością wymiany pojedynczego wentylatora w trakcie pracy urządzenia (ang. hot-swap).
4.	Przełącznik musi zostać dostarczony z następującymi interfejsami mogącymi działać równocześnie: ● 24 portów 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 10G-ER, 1G-LX, 1G-SX ● 6 portów 40G/100G QSFP28 z obsługą modułów 40G-SR, 40G-LR, 100G-CWDM4, 100G-FR1 Urządzenie musi umożliwiać w przyszłości zwiększenie przepustowości portów 40G do prędkości 100G poprzez zakup dodatkowej licencji bądź możliwość instalacji dodatkowego modułu z 6 portami 100G. W ramach postępowania Zamawiający wymaga dostarczenia takiej licencji bądź dodatkowego modułu z 6 portami 100G. Zamawiający nie dopuszcza aby realizacja portów 10G

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	była realizowana poprzez tzw. rozszywanie portów 10G/40G na 4 porty 10G. Wszystkie interfejsy 10G, 40G/100G muszą być dostępne z przodu obudowy.
5.	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) zarządzanie stosem poprzez jeden adres IP, b) minimum 8 jednostek w stosie, c) możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation), d) stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree, e) jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. Zamawiający dopuszcza aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink.
6.	Układ przełączający o wydajności min. 1,68 Tbps
7.	Obsługa min. 300 000 adresów MAC
8.	Wbudowana pamięć RAM min. 4 GB.
9.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 2 GB
10.	Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
11.	Możliwość skonfigurowania min. 1023 interfejsów vlan interface SVI działających równocześnie.
12.	Obsługa ramek jumbo o wielkości min. 9216 bajtów
13.	Obsługa mechanizmów ERPD
14.	Obsługa protokołu BFD oraz LACP
15.	Obsługa protokołu VRRP dla IPv4 i IPv6
16.	Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP). Wymagane wsparcie dla min. 63 instancji protokołu MSTP.
17.	Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-ISv6, BGPv4, BGPv4+, RIP, RIPng, PIM-SM, PIM-DM i SSM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
18.	Obsługa min. 256 000 tras dla routingu IPv4
19.	Obsługa min. 80 000 tras dla routingu IPv6
20.	Obsługa protokołów związanych z obsługą ruchu typu multicast: a) IGMP v1, v2 i v3

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	b) IGMP Snooping v1, v2 i v3 c) PIM-SM, PIM-DM, PIM-SSM
21.	Obsługa protokołów LLDP
22.	Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
23.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) min. 4 poziomy dostępu administracyjnego poprzez konsolę, b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL, c) możliwość utworzenia reguł ACL, d) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, a) zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 i SSHv2, e) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, porty TCP/UDP, f) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, g) obsługa mechanizmów związanych z ochroną protokołu STP: BPDU Protection, Root Protection, Loop Protection, h) możliwość synchronizacji czasu zgodnie z NTP IPv4.
24.	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: ● klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP, ● wsparcie dla mechanizmów QoS.
25.	Wymagane opcje zarządzania: a) możliwość lokalnej obserwacji ruchu na określonym porcie, b) 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), c) możliwość zarządzania urządzeniem z wykorzystaniem protokołu Netconf/Yang lub RESTCONF, d) wsparcie dla skyptów python uruchamianych na urządzeniu, e) wsparcie dla RMON, f) dedykowany port konsoli, zgodny ze standardem RS-232, g) dedykowany port zarządzający out-of-band Ethernet 10/100Base-T.
26.	Wraz z urządzeniami muszą zostać dostarczone: a) 2 wkładki QSFP28 100G kompatybilne z dostarczanym urządzeniem oraz niezbędne patchcordy światłowodowe min. 3 m,

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	b) 12 wkładek SFP+ 10GE SR kompatybilnych z dostarczanym urządzeniem oraz niezbędne patchcordy światłowodowe: 8 szt. patchcord światłowodowy 3 m; 4 szt. patchcord światłowodowy 5m, c) 10 wkładek SFP+ RJ-45 o przepustowości 10 / 100 / 1000 Mb/s kompatybilnych z dostarczanym urządzeniem, d) 2 wkładek SFP+ 10GE RJ-45 o przepustowości 10000 Mb/s kompatybilnych z dostarczanym urządzeniem, e) 12 patchcordów Ethernet kat.6 3 m, f) pełna dokumentacja w języku polskim lub angielskim, g) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.
27.	Wsparcie dla funkcjonalności VXLAN L2 i L3. Jeżeli obsługa powyższej funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający nie wymaga jej dostarczenia.
28.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
29.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
30.	Zamawiający wymaga, aby przełącznik posiadał 36 miesięcy serwis gwarancyjny świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.
31.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.

16. MOPS Wdrożenie domeny Microsoft AD

Opis

1. Instalacja 2 kontrolerów domeny:
   - jednego na maszyny wirtualnej na platformie HyperV,
   - drugiego na serwerze fizycznym.
1. Założenie kont użytkowników na podstawie dostarczonej listy w excelu.
2. Założenie podstawowych 10 grup i przypisanie użytkowników do grup.
3. Podłączenie maksymalnie 5 komputerów do domeny z migracją profilu.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

4. Dokumentacja.

17. MOPS Oprogramowanie do zarządzania tożsamością i dostępem - system operacyjny Windows Server 2022 Standard 16 Core License Pack lub równoważny

Opis

Wymagane minimalne parametry techniczne **oznaczające wymogi równoważne dla systemu Windows Server 2022 standard 16 core**	
Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Wymaga się dostarczenia 2 licencji na 16 rdzeni każda.	
Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy.	
1	Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym.
2	Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
3	Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
4	Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7	Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8	Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
9	Wbudowane wsparcie instalacji i pracy na wolumenach, które: • pozwalają na zmianę rozmiaru w czasie pracy systemu, • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, • umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, • umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10	Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

11	Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12	Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13	Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14	Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15	Graficzny interfejs użytkownika.
16	Zlokalizowane w języku polskim, następujące elementy: • menu, • przeglądarka internetowa, • pomoc, • komunikaty systemowe.
17	Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
18	Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
19	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
20	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
21	Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: • Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, • Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: - Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. • Zdalna dystrybucja oprogramowania na stacje robocze. • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej • Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: - Dystrybucję certyfikatów poprzez http, - Konsolidację CA dla wielu lasów domeny.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

	• Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. • Szyfrowanie plików i folderów. • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). • Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. • Serwis udostępniania stron WWW. • Wsparcie dla protokołu IP w wersji 6 (IPv6), • Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla: - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych, - Obsługi 4-KB sektorów dysków, - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra. • Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
22	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
23	Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
24	Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
25	Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

18. MOPS Zasilacz awaryjny stanowiskowy UPS

Opis

Lp.	Nazwa parametru	Wymagane minimalne parametry techniczne
1	Moc (VA / W)	700 VA / 360 W
2	Typ obudowy	Wieżowa (Tower)
3	Technologia	Line-Interactive

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

4	Układ automatycznej regulacji napięcia (AVR)	Tak
5	Napięcie znamionowe wejściowe	220 – 240 V
6	Zakres napięcia wejściowego bez użycia akumulatora	140 – 300 V
7	Napięcie wyjściowe	230 V (regulowane 220/230/240 V)
8	Zakres częstotliwości wejściowej	50 / 60 Hz (46 - 65 Hz zakres roboczy)
9	Czas przełączania	Maks. 10 ms dla przejścia z trybu normalnego do trybu bateryjnego
10	Sprawność	Min. 95% (przy pracy normalnej)
11	Przewód zasilający	Stały przewód z wtykiem CEE 7/7 (Unischuko)
12	Gniazda wyjścia	2x gniazda typu E (polskie z bolcem)
13	Czas podtrzymania dla obciążenia 240W	Min. 3 minut
14	Czas podtrzymania dla obciążenia 120W	Min. 12 minut
15	Zimny start	Tak
16	Automatyczny test baterii	Tak, automatyczny test baterii i alarm konieczności wymiany baterii
17	Port komunikacyjny	Tak, USB
18	Funkcja Auto-restartu	Tak, umożliwiająca automatyczne ponowne uruchomienie, gdy zasilanie sieciowe powróci po całkowitym rozładowaniu baterii.
19	Zarządzanie zasilaczem	Automatyczne połączenie z narzędziami zasilania w systemie Windows w celu bezpiecznego wyłączenia systemu.
20	Oprogramowanie dostarczone z UPS (lub dostępne do pobrania na stronie internetowej producenta)	Wymagane cechy oprogramowania: • Bezpieczne zamykanie systemów operacyjnych, • Dostęp do statusu pracy UPS i dziennika zdarzeń, • Analiza zużycia i kosztów energii, • Konfiguracja parametrów zasilacza UPS, • Automatyczne aktualizacje programu. Oprogramowanie kompatybilne z systemem Windows 10/11.
21	Stopień ochrony	IP20
22	Poziom hałasu	Maks. 25 dBA
23	Certyfikaty i zgodność z normami	IEC/EN 62040-1; IEC/EN 62040-2, IEC/EN 62040-3; CE lub równoważne
24	Gwarancja	Gwarancja realizowana przez serwis producenta min. 24 miesiące

19. MOPS Przełącznik sieciowy zarządzalny 24 porty

Opis

1. **Porty przełącznika**: minimum 24x 10/100/1000Base-T RJ45 oraz minimum 4x 100/1000Base-X SFP.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

2. **Port konsolowy:** RJ45 (RS-232).
3. **Port USB:** minimum 1 port co najmniej w standardzie 2.0.
4. **Szybkość przełączania:** minimum 56Gb/s.
5. **Przepustowość:** minimum 41Mp/s.
6. **Bufor pakietów:** minimum 1,5MB.
7. **Ramki Jumbo:** minimum 10k.
8. **Tablica adresów MAC:** minimum 16k.
9. **Adresy MAC – Multicast:** minimum 4k.
10. **Tablica ACL:** minimum 512.
11. **Tablica VLAN:** minimum 4k.
12. **Taktowanie procesora:** minimum 700MHz.
13. **Pamięć Flash:** minimum 32MB.
14. **Pamięć RAM:** minimum 256MB.
15. **Temperatura pracy:** zakres minimum 0°C - 50°C.
16. **Wilgotność względna:** zakres minimum 10% - 90% (bez kondensacji).
17. **Zasilanie:** zabudowany zasilacz 230V AC.
18. **Pobór mocy:** maksymalnie 21W.
19. **Wymiary:** RACK 1U.
20. **Certyfikaty bezpieczeństwa**: CE, RoHS lub równoważne
21. **VLAN:** Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ.
22. **DHCP:** IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server.
23. **Spanning tree:** IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Root Guard, BPDU guard.
24. **Protekcja ringowa:** ITU-T G.8032 ,Fast Link, Loopback Detection.
25. **Agregacja łączy:** IEEE 802.3ad (LACP), 16 groups per device / 8 ports per group, load balance.
26. **Bezpieczeństwo:** Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, ARP-Spoofing , Anti-ARP-Scan, ARP Binding, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, RADIUS, TACACS+.
27. **Multicast:** IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MLD v1/v2 Snooping
28. **QoS:** 8 Queues Per Port; Bandwidth Control; Flow Redirect; Classification based on ACL, VLAN ID, COS, TOS, DSCP; Policing Based on Port and VLAN; Single Rate single barrel double color for Policing; Remark DSCP, COS/802.1p, IP Precedence, TOS; Strict Priority, Weighted Round Robin, Strict priority in Weighted Round Robin, Weighted Deficit Round Robin for Scheduling, Match the IP fragmentation of message.
29. **Lista kontroli dostępu:** IP ACL, MAC ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, VLAN ACL.
30. **Diagnostyka:** sFlow, RSPAN, Ping, Trace Route, Dying GASP.
31. **Zarządzanie:** TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, UDLP (like UDLD), LLDP/LLDP MED VSF.
32. **Oprogramowanie oraz wsparcie techniczne:** oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

33. **Gwarancja:** lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

20. MOPS Przełącznik sieciowy zarządzalny 48 portów.

Opis

1. **Porty przełącznika**: minimum 48x 10/100/1000Base-T RJ45 oraz minimum 4x 100/1000Base-X SFP.
2. **Port konsolowy:** RJ45 (RS-232).
3. **Port USB:** minimum 1 port co najmniej w standardzie 2.0.
4. **Szybkość przełączania:** minimum 104Gb/s.
5. **Przepustowość:** minimum 77Mp/s.
6. **Bufor pakietów:** minimum 1,5MB.
7. **Ramki Jumbo:** minimum 10k.
8. **Tablica adresów MAC:** minimum 16k.
9. **Adresy MAC – Multicast:** minimum 2k.
10. **Tablica ACL:** minimum 2k.
11. **Tablica VLAN:** minimum 4k.
12. **Taktowanie procesora:** minimum 700MHz.
13. **Pamięć Flash:** minimum 32MB.
14. **Pamięć RAM:** minimum 128MB.
15. **Temperatura pracy:** zakres minimum 0°C - 50°C.
16. **Wilgotność względna:** zakres minimum 10% - 90% (bez kondensacji).
17. **Zasilanie:** zabudowany zasilacz 230V AC.
18. **Pobór mocy:** maksymalnie 41W.
19. **Wymiary:** RACK 1U.
20. **Certyfikaty bezpieczeństwa**: CE, RoHS lub równoważne
21. **VLAN:** Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Selective QinQ, Flexible QinQ.
22. **DHCP:** IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server.
23. **Spanning tree:** IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Root Guard, BPDU guard.
24. **Protekcja ringowa:** ITU-T G.8032 ,Fast Link, Loopback Detection.
25. **Agregacja łączy:** IEEE 802.3ad (LACP), 16 groups per device / 8 ports per group, load balance
26. **Bezpieczeństwo:** Storm Control based on packets and bytes, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting Radius, TACACS+.
27. **Multicast:** IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MLD v1/v2 Snooping
28. **QoS:** 8 queques per port, Bandwidth Control, Flow Control, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client.
29. **Lista kontroli dostępu:** IP ACL, MAC ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, VLAN ACL.
30. **Diagnostyka:** sFlow, RSPAN, Ping, Trace Route, Dying GASP.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

ZP.271.25.2024

31. **Zarządzanie:** TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, UDLP (like UDLD), LLDP/LLDP MED VSF.
32. **Oprogramowanie oraz wsparcie techniczne:** oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług.
33. **Gwarancja:** lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

21. Szkolenie specjalistyczne z obsługi UTMa

Cel szkolenia:

Celem kursu FortiGate - kompleksowa ochrona każdej sieci jest zaprezentowanie najczęściej stosowanych funkcji i metod zarządzania urządzeniami FortiGate firmy Fortinet. Zdobycie umiejętności samodzielnej konfiguracji poszczególnych modułów bezpieczeństwa takich, jak: AntyVirus, AntySpam, WebFilter, IPS. Poznanie funkcjonalności modułu umożliwiającego kontrolę aplikacji. Zaprezentowanie dostępnych rozwiązań VPN.
Szkolenie przeprowadzane w formie warsztatów ze znaczną liczbą praktycznych laboratoriów. Zakres tematyczny oraz część warsztatowa dostosowana zostanie do potrzeb uczestników szkolenia.
Szkolenie oparte jest o FortiOS w wersji 6.x.

Plan szkolenia:

1. Produkty - rodzaje, pozycjonowanie, wymiarowanie
2. Podstawowe czynności administracyjne:
   a) konfiguracja domyślna,
   b) update firmware,
   c) kopia zapasowa konfiguracji,
   d) serwisy,
   e) licencyjne.
3. Wstępna konfiguracja:
   a) tryby pracy,
   b) konfiguracja interfejsów sieciowych,
   c) konfiguracja serwera DHCP,
   d) dodatkowe ustawienia sieciowe,
   e) dostęp administracyjny.
4. Logowanie - metody logowania i ich praktyczna konfiguracja.
5. FortiAnalyzer.
6. Syslog.
7. Pamięć RAM.
8. Konfiguracja zapory ogniowej:
   a) elementy podstawowe,
   b) obiekty i grupy,

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

c) reguły zapory ogniowej,
d) translacja adresów SNAT i DNAT.

9. Uwierzytelnianie:
   a) metody uwierzytelniania użytkowników,
   b) lokalna baza użytkowników,
   c) grupy użytkowników.
10. Routing statyczny.
11. Ping Server – metryka i priorytety.
12. Zarządzanie zagrożeniami:
   a) moduł antywirusowy,
   b) moduł antyspamowy,
   c) filtrowanie stron WWW,
   d) kontrola aplikacji,
   e) moduł IPS i DLP.
13. Wirtualne Sieci Prywatne:
   a) VPN SSL,
   b) VPN vs IPSec VPN,
   c) konfiguracja tuneli VPN.

Wymagania:

Podstawowa znajomość TCP/IP oraz zagadnień bezpieczeństwa sieci.

Certyfikaty:

Uczestnicy szkolenia otrzymują **certyfikaty** wystawione imiennie oraz na Urząd sygnowane przez firmę szkolącą.

Projekt Cyberbezpieczny Samorząd dofinansowany jest ze środków Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa