WRiZP.272.4.3.2025

Załącznik Nr 3 do Projektu umowy
Opis przedmiotu zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ I : DYSKI WEWNĘTRZNE ORAZ ZEWNĘTRZNE

1. Dyski do macierzy [SP] – 10 sztuk

1.1. Dyski muszą być nowe, nie odnawiane, nie refabrykowane oraz muszą pochodzić z oficjalnej dystrybucji producenta.
1.2. Dyski muszą być w pełni kompatybilne z posiadaną przez Zamawiającego macierzą QSAN XS1212S+.
1.3. Format dysku: 3.5 cala.
1.4. Interfejs: SAS 12 Gbps.
1.5. Dopuszcza się zarówno tradycyjne dyski twarde (HDD) jak i dyski wykonane w technologii półprzewodnikowej (SSD).
1.6. Pojemność: co najmniej 22TB (niesformatowana).
1.7. Pamięć podręczna (cache): co najmniej 512 MB.
1.8. Prędkość obrotowa: co najmniej 7200 obr/min.
1.9. Ilość operacji wejścia/wyjścia (IOPS) dla próbki 4 KB przy odczycie: co najmniej 150.
1.10. Ilość operacji wejścia/wyjścia (IOPS) dla próbki 4 KB przy zapisie: co najmniej 500.
1.11. Prędkość transferu ciągłego: co najmniej 250 MB/s.
1.12. Średni czas pomiędzy awariami (MTBF): co najmniej 2 miliony godzin.
1.13. Gwarancja: co najmniej 5 lat.

2. Dyski serwerowe [SP]

2.1 Dyski – typ 1 – 16 sztuk

2.1.1. Dyski muszą być zgodne z posiadanymi przez Zamawiającego serwerami Dell PowerEdge R750 oraz zamontowanym w nich kontrolerem PERC H755. Service tagi serwerów: DYRXWT3, FYRXWT3.
2.1.2. Dyski muszą posiadać w zestawie wszelkie akcesoria montażowe (np. ramki lub szyny) umożliwiające ich instalację w serwerach opisanych w pkt 2.1.1. Zestaw montażowy musi obsługiwać funkcje powiadamiania o statusie dysku za pośrednictwem diody LED wbudowane w serwery opisane w pkt 2.1.1.
2.1.3. Dyski muszą być nowe, nie odnawiane, nie refabrykowane i muszą pochodzić z oficjalnej dystrybucji producenta.
2.1.4. Pojemność: co najmniej 2,4 TB (tzw. surowa, przed sformatowaniem)
2.1.5. Rozmiar: 2,5 cala
2.1.6. Interfejs: SAS 12 Gb/s
2.1.7. Dopuszczalne są dyski zarówno w technologii magnetycznej (HDD) jak i półprzewodnikowej (SSD).
2.1.8. Gwarancja: co najmniej 3 letnia gwarancja producenta

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

2.2 Dyski – typ 2 – 8 sztuk

2.2.1. Dyski muszą być zgodne z posiadanymi przez Zamawiającego serwerami Dell PowerEdge R750 oraz zamontowanym w nich kontrolerem PERC H755. Service tagi serwerów: DYRXWT3, FYRXWT3.
2.2.2. Dyski muszą posiadać w zestawie wszelkie akcesoria montażowe (np. ramki lub szyny) umożliwiające ich instalację w serwerach opisanych w pkt 2.2.1. Zestaw montażowy musi obsługiwać funkcje powiadamiania o statusie dysku za pośrednictwem diody LED wbudowane w serwery opisane w pkt 2.2.1.
2.2.3. Dyski muszą być nowe, nie odnawiane, nie refabrykowane i muszą pochodzić z oficjalnej dystrybucji producenta.
2.2.4. Pojemność: co najmniej 960 GB (tzw. surowa, przed sformatowaniem)
2.2.5. Rozmiar: 2,5 cala
2.2.6. Interfejs: SAS 12 Gb/s
2.2.7. Dopuszczalne są tylko dyski w technologii półprzewodnikowej (SSD).
2.2.8. Gwarancja: co najmniej 3 letnia gwarancja producenta.

3. Dyski zewnętrzne [SP] – 2 sztuki

3.1. Dyski muszą być nowe, nie odnawiane, nie refabrykowane oraz pochodzić z oficjalnej dystrybucji producenta.
3.2. Dysk w dedykowanej obudowie z interfejsem USB.
3.3. Dopuszczalne dyski zarówno w technologii magnetycznej (HDD) jak i półprzewodnikowej (SSD).
3.4. Pojemność: co najmniej 20 TB (niesformatowana, tzw. RAW).
3.5. Interfejs połączenia: USB 3.0 lub nowszy.
3.6. W zestawie przewód USB 3.0 zakończony z jednej strony wtyczką USB-A, a z drugiej wtyczką kompatybilną z obudową dysku.
3.7. Dopuszczalne są dyski zasilane z dodatkowego zasilacza. W takim wypadku zasilacz musi znajdować się w komplecie razem z dyskiem.
3.8. Gwarancja: co najmniej 2 letnia gwarancja.

4. Dysk zewnętrzny [DPS] – 1 sztuka

4.1. Rodzaj urządzenia
4.1.1. Macierz dyskowa
4.1.2. Min. 2 wnęki
4.1.3. wbudowane funkcje 256-bitowego szyfrowania sprzętowego AES
4.1.4. min. 2 porty hub USB 3.2 Gen min. 1 port USB 3.0 do podłączania akcesoriów komputerowych lub ładowania urządzeń mobilnych
4.1.5. dołączone oprogramowanie producenta: Security, Drive Utilities, Backup, Discovery
4.1.6. dołączone oprogramowanie umożliwiające tworzenie kopii zapasowych i klonowanie dysków.
4.1.7. Technologia RAID 0, RAID 1, JBOD
4.2. Pojemność dysków Min. 36 TB
4.3. Interfejs: Min. 1 USB 3.2 Gen. 1
4.4. Złącza: Min. 1 USB Typu-C
4.5. Złącza: Min. 2 USB Typu-A

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

4.6. Interfejs: Min. 1 USB 3.2 Gen. 1
4.7. Gwarancja minimum 2 lata

5. Dysk [PZEA] – 4 sztuki

5.1. Typ i zastosowanie: dysk twardy HDD
5.2. Format dysku: 3,5 cala
5.3. Pojemność dysku: min. 22TB
5.4. Prędkość obrotowa: min. 7200 rpm
5.5. Interfejs: SATA (III)
5.6. Szybkość transmisji interfejsu dysku twardego: 6 Gbit/s
5.7. Bufor: min. 512 MB
5.8. MTBF (Średni okres międzyawaryjny): 1000000 godz.
5.9. Limit obciążenia pracą: min. 300 TB/rok
5.10. Przeznaczenie: Serwer
5.11. Gwarancja: min. 5 lat

CZĘŚĆ II: SERWERY, SERWERY NAS ORAZ MACIERZE

6. Macierz [SP] – 1 sztuka

6.1. Obudowa: 2U z 12 zatokami na dyski, z szynami montażowymi w komplecie
6.2. Rozbudowa: Możliwa rozbudowa urządzenia do co najmniej 254 dysków (poprzez opcjonalne dołożenie jednostek rozszerzających). Zamawiający dopuszcza macierze z większą niż 12 ilością zatok na dyski, ale o wysokości 2U.
6.3. Gwarancja: co najmniej 2 lata gwarancji producenta NBD (Next Business Day - następnego dnia roboczego)
6.4. Wentylatory: co najmniej 2 sztuki hot swap lub dwa redundantne moduły wentylatora
6.5. Zasilanie: co najmniej dwa redundantne zasilacze o mocy pozwalającej na pracę na jednym zasilaczu w przypadku awarii jednego z nich
6.6. Kontrolery: Jeden kontroler sprzętowy. Możliwość dołożenia drugiego kontrolera (tryb pracy active-active).
6.7. System plików: Blokowy
6.8. Obsługa RAID: obsługa trybów RAID co najmniej 1, 5, 6, 10.
6.9. Obsługa: Globalny dysk zapasowy, dedykowany dysk zapasowy, możliwość utworzenia dodatkowych LUN, szybka odbudowa RAID, Thin Provisioning (w standardzie), możliwość obsługi SSD Cache & Auto Tiering, do 256 połączeń iSCSI
6.10. Cache kontrolera: co najmniej 4GB z obsługą funkcji copy-to-flash. Możliwość podłączenia modułu podtrzymania bateryjnego
6.11. Obsługa dysków:
6.11.1. 3.5" NL-SAS HDD
6.11.2. 2.5" SAS SSD
6.11.3. 2.5" SAS SED SSD
6.11.4. 2.5" SAS HDD
6.11.5. 2.5" SAS SED HDD

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

6.12. Dyski: urządzenie musi zostać dostarczone wraz z 10 sztukami dysków twardych zgodnych z urządzeniem o pojemności min 22 TB każdy.
6.13. Interfejsy: co najmniej dwa 10 GbE iSCSI RJ-45 (dopuszcza się zapewnienie tych interfejsów za pośrednictwem kart rozszerzających).
6.14. Urządzenie musi zapewniać możliwość dołożenia kart rozszerzających z portami 10GbE iSCSI SFP+
6.15. Złącze umożliwiające zdalne zarządzanie zgodne ze standardem Fast Ethernet lub szybszym.
6.16. Funkcje
6.16.1. Migawki,
6.16.2. klonowanie wolumenów,
6.16.3. thin provisioning,
6.16.4. zdalna replikacja,
6.16.5. Windows VSS,
6.16.6. LACP,
6.16.7. trunking, obsługa Jumbo frame,
6.16.8. narzędzie do sprawdzenia stanu nowo podłączonego dysku przed dodaniem go do wolumenu,
6.16.9. przechowywanie starszych konfiguracji z możliwością przywrócenia ich na macierz.
6.17. Wsparcie dla systemów: Co najmniej Windows Server 2019, 2022
6.18. Wyposażenie dodatkowe: 2x moduł optyczny Fibre Channel 16Gb/s SFP+, dostarczone wraz z urządzeniem

7. Serwer NAS [SOSW] – 1 sztuka

7.1. Urządzenie nowe, gwarancja 2 lata – wartość minimalna
7.2. Wartości minimalne:
7.2.1. Procesor - (4rdzenie/4wątki) 2700Mhz
7.2.2. Pamięć RAM - 4 GB (DDR4)
7.2.3. Rodzaje wyjść / wejść
7.2.4. USB 3.2 Gen. 1 - 2 szt.
7.2.5. RJ45 (LAN) 1 Gbps - 2 szt.
7.2.6. eSATA - 1 szt.
7.2.7. DC-in (wejście zasilania) - 1 szt.
7.2.8. Pojemność - 4x4TB HDD 5400obr/min
7.2.9. Wymagana obsługa RAID 1

8. Serwer NAS [ZSOiP] – 1 sztuka

8.1. Co najmniej czterordzeniowy procesor (o taktowaniu co najmniej 2,8 GHz).
8.2. Co najmniej dwa porty 2,5GbE RJ45.
8.3. Co najmniej gniazdo M.2 PCIe Gen3.
8.4. Co najmniej gniazdo PCIe Gen 3.
8.5. Karta sieciowa 10GbE/5GbE.
8.6. Pamięć RAM o co najmniej pojemności 8 GB.
8.7. Co najmniej wyjście HDMI 4K.
8.8. Dysk x 2 co najmniej 8TB do pracy ciągłej.
8.9. Nie krótsza gwarancja niż 3 lata, sprzęt nowy.
8.10. System operacyjny Linux.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

9. Serwer NAS [ZSS] – 1 sztuka

9.1. Wszystkie dostarczone urządzenia i podzespoły powinny być nowe, oryginalnie zapakowane, opatrzone pisemną gwarancją minimum dwa lata.
9.2. Serwer NAS powinien posiadać minimum dwa porty Gigabit RJ-45, które można ze sobą powiązać przy użyciu funkcji agregacji łączy Link Aggregation w celu zapewnienia automatycznego przełączania awaryjnego sieci i równoważenia obciążenia.
9.3. Na serwerze NAS powinny być dostępne usługi takie jak:
9.4. VPN Server obsługujący co najmniej protokoły VPN: PPTP, OpenVPN™, L2DTP/IPSec oraz minimalną liczbę połączeń w liczbie35.
9.5. Usługi katalogowe czyli łączenie się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/NFS/AFP/FTP/File przy użyciu istniejących poświadczeń.

10. Serwer NAS [DD] – 1 sztuka

10.1. Typ urządzenia: Serwer NAS
10.2. Obudowa: Tower
10.3. Procesor : Czterordzeniowy procesor o taktowaniu 2,0 GHz osiągający w teście PassMark co najmniej 2956 punktów
10.4. Sprzętowy mechanizm szyfrowania: Tak (AES-NI)
10.5. Pamięć RAM: min. 2 GB pamięci non ECC z możliwością rozszerzenia do min. 6 GB
10.6. Możliwości rozbudowy: Sprzęt powinien być wyposażony w min. 2 kieszenie na dyski twarde typu hot-swap
10.7. Dyski twarde: Sprzęt powinien być wyposażony w 2 dyski twarde 3,5’ SATA 6Gb/s, 256 MB Cache ,7200 RPM, o pojemności 6 TB każdy, dyski muszą być kompatybilne z urządzeniem, tj. wspierane przez jego producenta
10.8. Porty zewnętrzne: Minimum: 2 porty USB 3.2.1
10.9. Porty sieciowe: Minimum: 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
10.10. Funkcja Wake on LAN/WAN: Tak
10.11. Wentylator obudowy: Min. 1 wentylator 92 mm x 92 mm
10.12. Obsługiwane protokoły sieciowe: SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
10.13. Obsługiwane systemy plików minimum:
  10.13.1. Wewnętrzny: Btrfs, ext4
  10.13.2. Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
10.14. Obsługiwane typy macierzy RAID: Basic, JBOD, RAID 0, RAID 1,
10.15. Funkcja udostępniania plików: Minimalna liczba kont użytkowników: 2 048
10.16. Minimalna liczba grup użytkowników: 256
10.17. Minimalna liczba folderów współdzielonych: 256
10.18. Minimalna liczba jednoczesnych połączeń SMB/AFP/FTP: 500
10.19. Uprawnienia: Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
10.20. Oprogramowanie:
  10.20.1. Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23

lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych

10.20.2. Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów

10.20.3. Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.

10.21. Wykonawca udzieli gwarancji:

10.22. 2 lata na urządzenie główne

10.23. 5 lat na dyski twarde.

11. Serwer [PZD] – 1 sztuka

11.1. Serwer musi być nowy, nie odnawiany, nie naprawiany oraz musi pochodzić z legalnej dystrybucji producenta.

11.2. Serwer w obudowie Micro Tower lub Small Form Factor. Możliwość pracy zarówno w pozycji pionowej jak i poziomej.

11.3. Wymiary maksymalne (przy ustawieniu serwera poziomo): 16 cm x 27 cm x 26 cm (wysokość, szerokość, głębokość).

11.4. Serwer musi posiadać moduł TPM 2.0, musi posiadać oprogramowanie UEFI z funkcją Secure Boot oraz być zgodny z oprogramowaniem opisanym w punkcie 15 i 16.

11.5. Serwer musi posiadać możliwość montażu co najmniej 4 dysków w formacie 3,5 cala i z interfejsem SATA III, a także dysków 2,5” z zastosowaniem odpowiednich akcesoriów montażowych (kieszeń, klatka, sanki itp.).

11.6. Procesor musi posiadać wydajność co najmniej 11000 punktów w przetwarzaniu wielowątkowym oraz 3500 punktów w przetwarzaniu jednowątkowym według testu Passmark[1].

11.7. Procesor musi natywnie przetwarzać instrukcje zgodne z architekturą x86-64 i być z nią w pełni zgodny.

11.8. Serwer musi posiadać co najmniej 32 GB pamięci RAM dostosowanej do szybkości magistrali procesora, nie może ona ograniczać wydajności procesora.

11.9. Podsystem dyskowy serwera musi składać się z dwóch dysków SSD z interfejsem SATA lub NVMe o pojemności co najmniej 960 GB każdy (przed sformatowaniem, tzw. pojemność RAW) i pracujących w macierzy RAID 1.

[1] https://www.cpubenchmark.net/

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23

11.10. Serwer musi posiadać sprzętowy kontroler RAID (nie programowy, nie hybrydowy) obsługujący co najmniej tryby RAID 0, 1 oraz 10. Kontroler może być zarówno wbudowany w płytę główną jak i w postaci dodatkowej karty rozszerzeń.

11.11. Serwer musi posiadać komplet okablowania do podłączenia zarówno dysków jak i kontrolera RAID.

11.12. Serwer musi posiadać kartę sieciową zgodną z Gigabit Ethernet[2] z co najmniej dwoma portami w standardzie RJ45. Karta sieciowa może być zarówno wbudowana w płytę główną jak i w postaci dodatkowej karty rozszerzeń.

11.13. Serwer musi posiadać możliwość instalacji co najmniej jednej karty rozszerzeń ze złączem PCI Express 4.0 lub nowszym z magistralą o szerokości 4x lub większą. Dopuszcza się zarówno sloty o pełnej wysokości lub o obniżonej (tzw. karty low profile).

11.14. Serwer musi posiadać co najmniej 4 porty USB 3.0 lub nowsze z czego co najmniej jeden port musi znajdować się na przednim panelu serwera.

11.15. Ze względu na posiadanie przez Zamawiającego infrastruktury opartej o Active Directory, w tym kontroler domeny oraz komputery zarządzane z systemem Windows, wraz z serwerem Wykonawca musi dostarczyć spełniającą poniższe wymagania licencję na system Microsoft Windows Server 2025 Essentials lub na system równoważny opisany w pkt 16:

11.15.1. Licencja musi być nowa, nigdy wcześniej nie aktywowana oraz pochodzić z oficjalnej dystrybucji producenta.

11.15.2. Licencja musi być przeznaczona do użytku na serwerze dostarczonym przez Wykonawcę (licencja dedykowana dla tego producenta OEM lub uniwersalna).

11.15.3. Licencja musi być wieczysta.

11.16. Kryteria równoważności systemu Windows Server 2025 Essentials:

11.16.1. System musi posiadać możliwość podłączenia go do posiadanej przez Zamawiającego domeny Active Directory, a także skonfigurowanie go jako kontrolera tej domeny.

11.16.2. System musi posiadać możliwość zarządzania komputerami podłączonymi do posiadanej przez Zamawiającego domeny Active Directory, w tym logowanie użytkowników z tej domeny oraz wdrażanie ustawień Group Policy Object (GPO) oraz Group Policy Preference (GPP) przypisanych do tej domeny.

11.16.3. System musi poprawnie pracować na dostarczonym serwerze bez konieczności stosowania jego wirtualizacji.

11.16.4. System musi umożliwiać uruchomienie hypervisora typu 1 (baremetal) i uruchomienie na nim dowolnej liczby maszyn wirtualnych (na przykład z systemem z rodziny Linux) z tymże tylko jedna z maszyn wirtualnych może być aktywowana z użyciem licencji opisanej w pkt 15 (Windows Server 2025 Essentials).

11.16.5. System, w ramach licencji na niego, musi oferować możliwość uruchomienia dodatkowych usług serwerowych:

11.16.5.1. Serwer DNS z definiowaniem stref wyszukiwania do przodu oraz do tyłu oraz przekazywaniem zapytań do nieobsługiwanych domen do innych serwerów DNS

11.16.5.2. Serwer plików udostępniający zasoby sieciowe za pośrednictwem protokołów SMB2 oraz SMB3 na podstawie uprawnień nadawanych dla kont użytkowników Active Directory

11.16.5.3. Serwer RADIUS obsługujący żądania uwierzytelniania od oprogramowania i sprzętu dostawców firm trzecich

[2] IEEE 802.3ab 1000BASE-T

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

11.16.5.4. Usługę synchronizacji w czasie rzeczywistym plików użytkownika z komputera z katalogiem tego użytkownika na serwerze

11.16.5.5. Usługę utworzenia lokalnego centrum certyfikacji (CA, Certification Authority) opartego o infrastrukturę PKI (public key infrastructure – infrastruktura klucza publicznego) pozwalającego generować certyfikatu dla użytkowników oraz urządzeń.

11.17. Na dostarczony serwer wykonawca udziela 3 letniej gwarancji od momentu dostarczenia sprzętu, gwarancja musi spełniać poniższe wymagania:

11.17.1. Czas reakcji na usterkę lub awarię serwera: do 1 dnia roboczego.

11.17.2. Czas usunięcia usterki lub awarii serwera: do 3 dni roboczych.

11.17.3. Wszelkie naprawy gwarancyjne muszą być świadczone w miejscu użytkowania serwera (tzw. on-site).

11.17.4. Gwarancja musi obejmować zarówno części jak i robociznę.

W przypadku uszkodzenia nośnika danych i konieczności jego wymiany, Zamawiający zastrzega sobie możliwość zatrzymania uszkodzonych nośników danych (tzw. „keep your hard drive" lub „defective media retention").

CZĘŚĆ III: URZĄDZENIA UTM, SWITCHE, ROUTERY

12. Switch 10 Gbit Ethernet [SP] – 1 sztuka

12.1. Switch FortiSwitch FS-T1024E lub równoważne urządzenie o parametrach opisanych poniżej.

12.2. Switch musi posiadać co najmniej 24 porty w standardzie 10 Gbit Ethernet i ze złączem miedzianym RJ45

12.3. Gwarancja i wsparcie techniczne: co najmniej 1 rok w trybie 8x5, obejmujące dostęp do aktualizacji oprogramowania sprzętowego.

12.4. Całkowita przepustowość przełączania niemniejsza niż 800 Gbps

12.5. Całkowita ilość przełączanych pakietów (dla rozmiaru pakietu 64 bajty) niemniejsza niż 1200 Mpps

12.6. Obudowa 1U dostosowana do montażu w szafie rack, wraz z urządzeniem muszą zostać dostarczone wszelkie akcesoria montażowe (np. uchwyty).

12.7. Możliwość zarządzania urządzeniem co najmniej w poniższym zakresie z poziomu posiadanych przez Zamawiającego urządzeń FortiGate 201F:

12.7.1. Automatyczne wykrywanie switcha przez urządzenia zarządzające oraz jego autoryzacja

12.7.2. Aktualizacja oprogramowania urządzenia

12.7.3. Ponowne uruchomienie urządzenia

12.7.4. Tworzenie i zarządzanie sieciami VLAN na portach urządzenia

12.7.5. Możliwość przydzielania zasad i zarządzania ruchem sieciowym dla VLANów obsługiwanych przez switch

12.8. Obsługa co najmniej poniższych funkcji i standardów sieciowych:

12.8.1. Obsługa co najmniej 255 VLANów

12.8.2. Możliwość przechowywania co najmniej 4 tysięcy wpisów w tablicy adresów MAC

12.8.3. LLDP/MED.

12.8.4. Spanning Tree

12.8.5. 802.1X Authentication (Port-based, MAC-Based, MAB)

12.8.6. Blokowanie ruchu pomiędzy VLANami

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

12.8.7. IEEE 802.1AX Link Aggregation
12.8.8. IEEE 802.3ad Link Aggregation with LACP
12.8.9. IEEE 802.1Q VLAN Tagging
12.8.10. IEEE 802.3ab 1000Base-T
12.8.11. IEEE 802.3ae 10 Gigabit Ethernet
12.8.12. Ramki Jumbo

13. Switch 8 port- przełącznik zarządzalny [I LO] – 1 sztuka

13.1. minimalna ilość portów 10G SFP+ - 2
13.2. minimalna ilość portów 1G RJ45 POE+ 6 oraz 2 POE++ (60W)
13.3. minimalna zdolność przełączania - 56 Gbps
13.4. Łączna dostępna moc portów PoE - minimum 120W
13.5. Obsługa L2: IGMP Snooping, STP/RSTP, Port isolation, Storm Control, Voice VLAN, Port Mirroring LACP, Flow Control, Jumbo Frames, DHCP snooping, 802.1X control
13.6. Obsługa L3: DHCP, DHCP Relay, Inter-Vlan routing, Static Routing
13.7. Gwarancja 2 lata

14. Switch 24 port- przełącznik zarządzalny [I LO] – 1 sztuka

14.1. minimalna ilość portów 1/10G SFP+ - 2
14.2. minimalna ilość portów 24G RJ45 POE+ 16 oraz 8 POE++ (60W)
14.3. minimalna zdolność przełączania - 88 Gbps
14.4. Łączna dostępna moc portów POE - min 400W
14.5. Zabezpieczenie ESD/EMP.
14.6. Obsługa L2: IGMP Snooping, STP/RSTP, Port isolation, Storm Control, Voice VLAN, Port Mirroring LACP, Flow Control, Jumbo Frames, DHCP snooping, LLDP-MED, 802.1X control
14.7. Obsługa L3: DHCP, DHCP Relay, Inter-Vlan routing, Static Routing, ACL
14.8. Gwarancja 2 lata

15. Firewall [I LO] – 1 sztuka

15.1. min 8 portów 1G Ethernet
15.2. min 1 port 2,5G Ethernet
15.3. min 2 porty SFP+ 10G
15.4. min 2 porty POE+ oraz 6 portów POE
15.5. Procesor min 4 rdzenie 1,7 GHz
15.6. Pamięć min 4 GB DDR4
15.7. Interfejs zarządzania Ethernet lub Bluetooth
15.8. Ochrona ESD/EMP.
15.9. Wbudowany zasilacz sieciowy.
15.10. Możliwość zamontowania w szafie rack.
15.11. Gwarancja 2 lata.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

16. Sprzętowa zapora ogniowa [PPP] – 1 sztuka

16.1. WYDAJNOŚĆ
16.1.1. Przepustowość Firewall (1518 bajtów UDP) minimum 2 Gbps
16.1.2. Przepustowość IPS (1518 bajtów UDP) minimum 1 Gbps
16.1.3. Przepustowość IPS (plik HTTP 1MB) minimum 500 Mbps
16.1.4. Przepustowość Antywirus minimum 500 Mbps
16.2. VPN*
16.2.1. Przepustowość IPSec - AES-GCM minimum 500 Mbps
16.2.2. liczba tuneli IPSec VPN minimum 20
16.2.3. liczba SSL VPN (tryb Portal) minimum 20
16.2.4. Liczba jednoczesnych klientów SSL VPN minimum 20
16.3. POŁĄCZENIA SIECIOWE
16.3.1. Liczba jednoczesnych sesji minimum 100,000
16.3.2. Nowe sesje na sekundę minimum 10,000
16.3.3. Liczba bram głównych/zapasowych minimum 5/5
16.3.4. INTERFEJSY SIECIOWE
16.3.5. Interfejsy Ethernet 100/1000/2500 minimum 4
16.3.6. Interfejsy światłowodowe 1Gb minimum2
16.4. SYSTEM
16.4.1. Liczba reguł filtrowania minimum 1024/4096
16.4.2. Liczba tras statycznych minimum 128
16.4.3. Liczba tras dynamicznych minimum 2000
16.5. REDUNDANCJA
16.5.1. High availability (active/passive)
16.5.2. Redundantne zasilanie Zewnętrzny zasilacz
16.6. SPRZĘT
16.6.1. Pamięć lokalna Karta MicroSD lub podobna
16.6.2. Partycja na logi Tak
16.6.3. Układ TPM
16.6.4. MTBF w 25°C (lata) minimum 10
16.7. CERTYFIKACJA
16.7.1. Zgodność CE (Conformité Européenne)
16.7.2. Zgodność CB (IEC System of Conformity Testing an Certification of Electrical Equipment and Components)
16.8. Gwarancja minimum 2 lata

17. Przełącznik 48 portowy zarządzalny [PPP] – 1 sztuka

17.1. Przełącznik L2+
17.2. 48 portów PoE+ Gigabit Ethernet RJ-45 z budżetem mocy minimum 200W
17.3. Minimum 2 porty 10Gigabit Ethernet SFP+
17.4. Konfiguracja VLAN oparta na portach, tagach 802.1Q, adresach MAC oraz protokołach
17.5. Voice VLAN oraz Surveillance VLAN w celu optymalizacji jakości połączeń oraz wideo

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

17.6. Bezpieczna sieć lokalna dzięki zabezpieczeniom portu 802.1x, ACL, IP Source Guard oraz DHCP Snooping
17.7. Obsługa IPv6 z MLD Snooping, IPv6 ACL oraz IPv6 DNS Resolver
17.8. Uwierzytelnianie przez lokalną bazę danych, serwery RADIUS oraz TACACS+
17.9. Zgodny z IEEE 802.3az (Energy-Efficient Ethernet)
17.10. Wsparcie SNMP v1/v2c/v3, RMON oraz Syslog do monitorowania sieci
17.11. Gwarancja minimum 2 lata

18. Urządzenie UTM do sieci bezprzewodowej [SOSW] – 1 sztuka

18.1. Urządzenie nowe, gwarancja 2 lata – wartość minimalna
18.2. Wartości minimalne:
18.2.1. Przepustowość IPS - 1 Gbps
18.2.2. Przepustowość NGFW - 800 Mbps
18.2.3. Przepustowość Threat Protection - 600 Mbps
18.2.4. Przepustowość zapory (Pakiety na sekundę) - 7.5 Mpps
18.2.5. Opóźnienie zapory (64 bajtowe pakiety UDP) - 3,3 µs
18.2.6. Sesje równoległe (TCP) - 700000
18.2.7. Nowe sesje na sekundę (TCP) - 35000
18.2.8. Przepustowość IPsec VPN (512 bajtów) - 4.4 Gbps
18.2.9. Przepustowość SSL-VPN - 490 Mbps
18.2.10. Liczba użytkowników SSL-VPN - 200
18.2.11. Przepustowość Kontroli SSL (IPS, HTTPS) - 310 Mbps
18.2.12. Inspekcja SSL CPS (IPS, HTTPS) - 320
18.2.13. Przepustowość CAPWAP (HTTP 64K) - 3.5 Gbps
18.2.14. Przepustowość kontroli aplikacji (HTTP 64K) - 990 Mbps
18.2.15. Interfejs bezprzewodowy - (2.4 GHz/5 GHz), 802.11/a/b/g/n/ac-W2
18.2.16. Liczba anten - 2 zewnętrzne
18.2.17. Porty
18.2.18. 3 x GE RJ-45
18.2.19. 1 x GE RJ-45 WAN
18.2.20. 1 x Konsola RJ-45
18.2.21. Sesja równoległa kontroli SSL - 55000
18.2.22. Pakiet bezpieczeństwa - licencja 3 lata minimum: monitorowanie ruchu sieciowego Ochrona antyspamowa, antywirusowa, ips, vpn, filtrURL

19. Urządzenie UTM [DD] – 1 sztuka

19.1. Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę 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 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

19.2 Redundancja, monitoring i wykrywanie awarii

19.2.1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.

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

19.2.3 Monitoring stanu realizowanych połączeń VPN.

19.2.4 System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

19.3 Interfejsy, Dysk, Zasilanie:

19.3.1 System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

- 5 portami Gigabit Ethernet RJ-45.

19.3.2 System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.

19.4 Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1 Gbps.
6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

19.5 Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są 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 .
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

19.6 Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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 istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

19.7 Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

- 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.
- Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
- Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
- Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
- Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

19.8 Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

19.9 Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

19.10 Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

19.11 Ochrona przed malware

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

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

19.12 Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
7. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

19.13 Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

19.14 Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

19.15 Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia 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. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

19.16 Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

19.17 Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

19.18 Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 2 lat.

19.19 Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 2 lat, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.

20. Router [DPS] – 1 sztuka

20.1. Rodzaj urządzenia
- 20.1.1. Router bezprzewodowy z modemem 5G, x DSL
- 20.1.2. Min. 2 Gniazda kart nano SIM,
- 20.1.3. IPSec, Klient VPN Open VPN, L2TP, PPTP, WireGuard

20.2. Obsługiwane standardy IEE 802.11n,

20.3. Zabezpieczenia transmisji bezprzewodowej WPA-PSK, WPA2-PSK, WPA3-SAE

20.4. Częstotliwość pracy Działanie dwuzakresowe z jednoczesną transmisja na pasmach 2,4 GHz i 5 GHZ

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

20.5. Rodzaje wejść: Min. 1 RJ-45 10/100/1000 (LAN/WAN)
20.6. Rodzaje wyjść: Min. 3 RJ-45 10/100/1000 (LAN)
20.7. Pasma transmisji 3G/4G: LTE: 700/800/850/900/1500/1800/2100/2600 MHz
20.8. Dodatkowe funkcje
20.8.1. DHCP
20.8.2. NAT
20.8.3. Filtrowanie adresów MAC
20.8.4. Zapora sieciowa
20.9. Automatyczne IP, DMZ, Dual WAN, Przekierowanie portów, Przekierowywanie NAT, Statyczne IP, UPnP
20.10. Gwarancja minimum 2 lata

21. Switch [DPS] – 5 sztuk

21.1. Rodzaj urządzenia
21.1.1. Switch
21.1.2. IEEE 802.1p, IEEE 802.1q, IEEE 802.3, IEEE 802.3ab, IEEE 802.3u, IEEE 802.3x
21.1.3. Minimalna liczba portów PoE – 8 szt.
21.1.4. Algorytm przełączania: Store and forward
21.1.5. Szybkość przekierowań pakietów: min. 23.0 Mb/s
21.2. Architektura sieci: Gigabit Ethernet
21.3. Całkowita liczba portów: Minimum 16
21.4. Obsługiwane standardy
21.4.1. IEEE 802.3
21.4.2. IEEE 802.3 u
21.4.3. IEEE 802.3 x
21.4.4. IEEE 802.3 ab
21.4.5. IEEE 802.1 p
21.4.6. IEEE 802.1 Q
21.5. Przepustowość: Min. 32 GB/s
21.6. Bufor pamięci: Min. 512 kb
21.7. Dodatkowe funkcje: Automatyczne krosowanie portów (Auto MDI-MDIX)
21.8. Dodatkowe funkcje: Automatyczna negocjacja szybkości połączeń
21.9. Gwarancja minimum 2 lata

22. Urządzenie UTM [PZD] – 1 sztuka

Ze względu na wykorzystywanie już przez jednostkę urządzeń marki FortiGate oraz zamiar połączenia tych urządzeń oraz kupowanego sprzętu tunelem VPN, a co za tym idzie zapewnienie ich kompatybilności wymagane jest urządzenie FortiGate 40F wraz z licencjami FortiCare Premium and FortiGuard Unified Threat Protection (UTP) na 1 rok lub urządzenie równoważne o parametrach opisanych poniżej.

Urządzenie musi być nowe, nie odnawiane, nie refabrykowane oraz musi pochodzić z oficjalnej dystrybucji producenta.

Gwarancja: co najmniej 1 rok.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

22.1. Zgodność

Urządzenie musi gwarantować pełną zgodność z użytkowanymi już przez Zamawiającego urządzeniami Fortigate 201F w zakresie zestawiania połączeń VPN IPSec IKEv2 w trybach zarówno site-to-site jak i client-to-site.

22.2. Redundancja, monitoring i wykrywanie awarii

1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
2. Monitoring stanu realizowanych połączeń VPN.
3. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

22.3. Interfejsy:

1. System musi posiadać co najmniej 4 porty RJ45 zgodne z Gigatbit Ethernet, które mogą być użytkowane do podłączania urządzeń sieci LAN Zamawiającego.
2. System musi posiadać co najmniej 1 port RJ45 zgodny z Gigatbit Ethernet, który może być użytkowany do podłączenia sieci rozległej (WAN) od dostawcy łącza internetowego.
3. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania oraz import/eksport konfiguracji z/do nośnika danych USB.
4. W ramach systemu Firewall powinna być możliwość zdefiniowania interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

22.4. Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 100 tys. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

22.5. Funkcje systemu bezpieczeństwa:

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.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

22.6. Polityki, Firewall

1. Polityka Firewall uwzględnia adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   2.1. Translację jeden do jeden oraz jeden do wielu.
   2.2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

22.7. Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   1.1. Wsparcie dla IKE v1 oraz v2.
   1.2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   1.3. Obsługa protokołu Diffie-Hellman grup 19 i 20.
   1.4. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   1.5. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   1.6. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   1.7. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   1.8. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23

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

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

2.3. Producent rozwiązania dostarcza oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

22.8. Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

1.1. Routingu statycznego.

1.2. Policy Based Routingu.

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

22.9. 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.

22.10. Ochrona przed złośliwym oprogramowaniem

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.

22.11. 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 być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

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 webowych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

22.12. 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 być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe 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.

22.13. 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. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
4. Funkcja wymuszania trybu Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
6. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

22.14. Uwierzytelnianie użytkowników w ramach sesji

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

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

1.2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDA

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

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

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

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

4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

22.15. 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.
5. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
6. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

22.16. Logowanie

1. 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.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

22.17. Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikacje ICSA lub EAL4 dla funkcji Firewall.

CZĘŚĆ IV: ZASILACZE UPS

23. Zasilacze UPS [SP] – 22 sztuki

23.1. Ilość: 22 sztuki

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

23.2. Zasilacz UPS do użytku biurowego musi posiadać moc co najmniej 390W/650VA oraz musi być przystosowany do pracy w sieci elektrycznej o napięciu 230V stosowanej w Polsce, a także musi posiadać następujące certyfikacje:

23.3. Certyfikat dopuszczenia do użytku na terenie Unii Europejskiej (tzw. certyfikat zgodności CE).

23.4. Certyfikat zgodności z dyrektywą ws. sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia 2014/35/EU (tzw. LVD – Low Voltage Directive)

23.5. Certyfikat zgodności z dyrektywą w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej 2014/30/WE (tzw. EMC – Electromagnetic Directive)

23.6. Certyfikat zgodności z dyrektywą w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym 2011/65/UE, wraz z późniejszymi zmianami (tzw. RoHS 3 – Restriction of Hazardous Substances)

23.7. Zasilacz musi podtrzymać zasilanie urządzeń do niego podłączonych i pobierających łącznie 60W przez co najmniej 30 minut.

23.8. Wraz z zasilaczem musi być dostarczony oryginalny akumulator o pojemności dostosowanej do mocy zasilacza UPS opisanej w pkt 2 oraz czasu podtrzymania opisanego w pkt 7.

23.9. Konstrukcja zasilacza UPS musi pozwalać na wymianę akumulatora przez użytkownika i bez użycia narzędzi.

23.10. Zasilacz musi być podłączany do zewnętrznego źródła zasilania przewodem zakończonym wtyczką typu francuskiego (wtyczka z otworem na bolec uziemienia). Dopuszcza się wtyczkę kombinowaną – połączenie wtyczki francuskiej z wtyczką typu Schuko. Przewód zasilający musi mieć długość co najmniej 1,5m.

23.11. Jeśli przewód zasilający ma możliwość jego odłączania od zasilacza UPS to zasilacz musi posiadać wejściowe złącze zasilania IEC C14, a przewód musi posiadać z jednej strony wtyczkę IEC C13, a z drugiej strony wtyczkę typu francuskiego (wtyczka z otworem na bolec uziemienia) lub kombinowaną wtyczkę typu francuskiego i Schuko.

23.12. Zasilacz musi posiadać co najmniej 4 gniazda typu francuskiego (tzw. z bolcem) z ochroną przed przepięciami oraz z podtrzymaniem zasilania. Dopuszcza się gniazda kombinowane – połączenie gniazd francuskich z gniazdami typu Schuko.

23.13. Zasilacz musi posiadać dwa gniazda RJ45 (jedno wejście, jedno wyjście) obsługujące ruch sieciowy Ethernet i zabezpieczające przed przepięciami.

23.14. Zasilacz musi posiadać gniazdo USB do podłączenia do komputera lub serwera pozwalające monitorować parametry zasilacza UPS. Gniazdo musi umożliwiać monitorowanie poziomu baterii oraz statusu ładowanie/rozładowywanie za pomocą funkcji wbudowanych w system Windows 10 oraz nowsze, bez konieczności instalowania dodatkowego oprogramowania. W zestawie musi znajdować się odpowiedni przewód zakończony z jednej strony wtyczką typu USB-A (po stronie komputera/serwera), a z drugiej strony wtyczką dostosowaną do zasilacza UPS.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23

23.15. Zasilacz musi posiadać co najmniej dwa gniazda USB ze złączem USB-A umożliwiające ładowanie urządzeń do niego podłączonych (np. smartfonów, tabletów itp.).

23.16. Zasilacz musi posiadać możliwość montażu na ścianie lub pod biurkiem. Jeśli w tym celu konieczne jest zastosowanie dodatkowego uchwytu to musi on zostać dostarczony razem z zasilaczem UPS.

23.17. Zasilacz UPS musi posiadać możliwość tzw. zimnego startu czyli włączenia podłączonych do niego urządzeń wyłącznie na zasilaniu bateryjnym, pod warunkiem że stopień naładowania akumulatora na to pozwala.

23.18. Zasilacz UPS musi posiadać zabezpieczenie przed głębokim rozładowaniem akumulatora.

23.19. Zasilacz musi posiadać sygnalizację dźwiękową (np. brzęczykiem) oraz sygnalizację wizualną (np. wyświetlacz LED/LCD lub diodę LED) informujące o przejściu na zasilanie bateryjne oraz o problemach w działaniu zasilacza takich jak awaria akumulatora lub przeciążenie.

23.20. Gwarancja minimum 2 letnia obejmująca również akumulator.

Projekt współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC),
Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa,
konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23