*Załącznik Nr 2 C do SIWZ*

Znak sprawy: ZP. 272.1.2020

**OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)**

**I. Przedmiot zamówienia**

1. Nazwa zamówienia: „Dostawa sprzętu komputerowego, serwerowego, sieciowego oraz zestawów komputerowych i urządzeń urządzeń peryferyjnych dla Powiatu Zduńskowolskiego” w ramach Części III pn. "Zakup i dostawa urządzeń sieci teleinformatycznej, infrastruktury przetwarzania danych oraz serwerowego systemu operacyjnego dla Powiatu Zduńskowolskiego".
2. Przedmiotem zamówienia jest dostawa fabrycznie nowych urządzeń, oprogramowania oraz wykonanie wszystkich niezbędnych usług instalacyjnych i konfiguracyjnych zgodnie ze sztuką, zaleceniami producenta i najlepszymi praktykami, koniecznych by dostarczone urządzenia poprawnie funkcjonowały w środowisku sieciowym Zamawiającego i zapewniały bezusterkową pracę użytkownikom Zamawiającego oraz przeprowadzenie szkoleń z zakresu konfiguracji i zarządzania systemem serwerowym, konfiguracji i zarządzania kopii bezpieczeństwa oraz konfiguracji i zarządzania bezpieczeństwem informacji.

3. W ramach realizacji zamówienia Części III wymaga się realizacji i dostawy, instalacji i konfiguracji:

1) Macierz – 1 komplet,
2) NAS – 1 komplet,
3) Sewery – 3 komplety,
4) Serwerowy system operacyjny – 3 komplet.,
5) Kontroler sieci bezprzewodowej – 1 komplet,
6) Acess Point – 10 kompletów,
7) Przełączniki dostępowe – 11 kompletów;
8) Zabezpieczenie styku z Internetem – 1 komplet

oraz przeprowadzenia z szkoleń z zakresu:

- konfiguracji i zarządzania systemem serwerowym dla 2 osób;
- konfiguracji i zarządzania kopii bezpieczeństwa dla 2 osób;
- konfiguracji i zarządzania bezpieczeństwem informacji dla 2 osób;

3. Miejscem dostawy jest budynek Starostwa Powiatowego w Zduńskiej Woli na:

Złotnickiego 25 budynek A , Zduńska Wola – PD_1

Złotnickiego 25 budynek B , Zduńska Wola – PD_2

Królewska 10, Zduńska Wola – PD_3

Żeromskiego 10a, Zduńska Wola – PD_4

**II. Termin wykonania zamówienia**

Wykonawca zobowiązuje się wykonać przedmiot zamówienia dla Części III w terminie 45 dni kalendarzowych licząc od dnia podpisania umowy.

**III. Wymagania ogólne dla dostarczanego przedmiotu zamówienia:**

1. Przedmiot zamówienia dostarczony i uruchomiony w ramach niniejszego zamówienia musi funkcjonować zgodnie z obowiązującymi w Polsce przepisami prawa.
2. Zamawiający wymaga, o ile zapisy OPZ nie stanowią inaczej, udzielenia bezterminowej, niewyłącznej licencji na korzystanie z dostarczonego przedmiotu zamówienia.
3. Dostarczany sprzęt i oprogramowanie musi pochodzić z autoryzowanego kanału sprzedaży producentów,
4. Zamawiający wymaga, by dostarczone urządzenia były nowe oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania),
5. Wykonawca zapewnia, że korzystanie przez Zamawiającego z zaoferowanych produktów nie będzie stanowić naruszenia praw majątkowych osób trzecich,
6. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone do wycofania ze

sprzedaży,

7. Oferowane oprogramowanie w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji, sprzedaży lub wsparcia technicznego,
8. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień poprzedzający dzień składania ofert.
9. Dla dostarczonego oprogramowania, o którym mowa w niniejszym Opisie Przedmiotu Zamówienia należy dostarczyć certyfikaty potwierdzające legalność użytkowania
10. Określone przez Zamawiającego w niniejszym Opisie Przedmiotu Zamówienia wymagania są wymaganiami minimalnymi,
11. Podane długości okresów trwania gwarancji w poszczególnych opisach sprzętu są okresami minimalnymi.

**IV. Wymagania w zakresie ochrony danych osobowych**

Przedmiot zamówienia dostarczony i uruchomiony w ramach niniejszego zamówienia musi funkcjonować zgodnie z obowiązującymi w Polsce przepisami prawa w zakresie ochrony danych osobowych.

Wykonawca zobowiązuje się do utrzymania tajemnicy o przetwarzanych w oprogramowaniu danych i nie ujawni danych osobowych, do których miał dostęp osobom trzecim, zarówno w czasie trwania umowy, jak i po jej wygaśnięciu.

**Serwer – 3 sztuki**

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa serwerów do siedziby Zamawiającego, spełniających minimalne wymagania techniczne i funkcjonalne określone poniżej oraz ich zamontowanie we wskazanym przez Zamawiającego miejscu, a także wykonanie wszystkich niezbędnych usług instalacyjnych i konfiguracyjnych (zainstalowanie serwerowego systemu operacyjnego, o którym mowa w niżej, sterowników, dysków, skonfigurowanie macierzy, umieszczenie w szafie rack, wpięcie do istniejącej sieci informatycznej Zamawiającego), zgodnie ze sztuką, zaleceniami producenta, wskazaniami Zamawiającego oraz najlepszymi praktykami,

koniecznych by dostarczone urządzenia po-prawnie funkcjonowały w środowisku informatycznym Zamawiającego i zapewniały wydajną i bezawaryjną pracę użytkownikom końcowym.

**Wymagane minimalne parametry techniczne:**

W celu instalacji i uruchomienia wszystkich planowanych do wdrożenia aplikacji i usług planuje się, zakup 3 serwerów. Serwery powinny spełniać następujące minimalne warunki:

- obudowa do montażu w szafie typu rack o wysokości max 2U;
- zasilanie redundantne, przynajmniej 2 zasilacze typu HotPlug; zasilacze o sprawności 90% o mocy niezbędnej do prawidłowego funkcjonowania serwera.
- płyta główna z możliwością zainstalowania minimum dwóch procesorów;
- zainstalowane procesory minimum ośmiordzeniowe klasy x86 dedykowane do pracy w serwerach, zaprojektowane do pracy w układach wieloprocesorowych; Procesory muszą być dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 72.6 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
- pamięć min 128 GB ECC RDIMM, rozszerzalna z zabezpieczeniem typu ECC.
- sprzętowy kontroler dyskowy, umożliwiający obsługę dysków z prędkościami transferu 12 Gb/s; umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej zabezpieczeń RAID: 0, 1, 5, 6, 10, 50, 60, wyposażony w wbudowaną, nieulotną pamięć cache o pojemności min. 2GB;
- dyski minimum 2x 600 GB typu SAS pracujące w RAID1;
- sieć minimum 4 x Ethernet 10Gb (w tym 2x10 Gb/s Ethernet w standardzie BaseT, 2x10GbE SFP+).
- Gwarancja:
    a. gwarancja producenta na okres 36 miesięcy świadczona na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego

    b. oświadczenie, że w przypadku awarii dysk twardy zostaje u Zamawiającego.

Ze względu na posiadaną przez Zamawiającego licencję oprogramowania bazodanowego liczba procesorów w **JEDNYM komplecie** serwera nie może przekroczyć 1, a liczba rdzeni procesora nie może przekroczyć 8. Pozostałe komplety serwerów winny mieć zainstalowane po dwie sztuki procesorów o parametrach opisanych w minimalnych warunkach.

**Macierz dyskowa 1 komplet**

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa macierzy do siedziby Zamawiającego, spełniających minimalne wymagania techniczne i funkcjonalne określone poniżej oraz ich zamontowanie we wskazanym przez Zamawiającego miejscu, a także wykonanie wszystkich niezbędnych usług instalacyjnych i konfiguracyjnych (zainstalowanie w szafie rack, skonfigurowanie RAID, wpięcie do istniejącej sieci informatycznej Zamawiającego), zgodnie ze sztuką, zaleceniami producenta, wskazaniami Zamawiającego oraz najlepszymi praktykami, koniecznych by dostarczone urządzenia poprawnie funkcjonowały w środowisku informatycznym Zamawiającego i zapewniały wydajną i bezawaryjną pracę użytkownikom końcowym.

**Wymagane minimalne parametry techniczne:**

- sprzętowa macierz dyskowa w obudowie typu rack; Może zajmować maksymalnie 2U
- umożliwiająca skonfigurowanie zabezpieczeń RAID: 0, 1, 5, 6, 10
- wyposażona w wbudowaną, nieulotną pamięć cache o pojemności min. 16 GB;
- dyski: minimum 8 x 4TB NLSAS oraz 4x960GB SSD SAS
- obsługa dysków z prędkościami 12 Gb/s;
- sieć: minimum 4 x interfejsy 16Gb/s i 4 interfejsy 10Gb/s
- Gwarancja:
    a. gwarancja producenta na okres 36 miesięcy świadczona na miejscu u klienta
       Czas reakcji serwisu - do końca następnego dnia roboczego
    b. Oświadczenie, że w przypadku awarii dysk twardy zostaje u Zamawiającego.

**Przełączniki dostępowe 11 kompletów**

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa przełączników do siedziby Zamawiającego, spełniających minimalne wymagania techniczne i funkcjonalne określonych poniżej oraz ich rozmieszczenie, a także wykonanie wszystkich niezbędnych usług instalacyjnych i konfiguracyjnych, zgodnie ze sztuką, zaleceniami producenta i najlepszymi praktykami, koniecznych by dostarczone urządzenia poprawnie funkcjonowały w środowisku sieciowym Zamawiającego i zapewniały bezusterkową pracę użytkownikom.

**Wymagane minimalne parametry techniczne:**

Przełączniki winny zapewnienić podłączenia do sieci LAN istniejących oraz nowo zakupionych komputerów. Przełączniki sieciowe winny być zarządzalne . Przełączniki zostały podzielone na 3 typy A,B,C. Urządzenia winny posiadać następujące minimalne funkcjonalności:

**Minimalne wymagania dotyczące wszystkich typów przełączników:**

- obsługa przełączania L2, w miarę możliwości L3
- możliwość zarządzania i konfiguracji poprzez sieć
- obsługa VLAN, filtrowanie ruchu

**Przełącznik TYP A szt. 1**

Wymaga się aby urządzenie minimalnie obsługiwało następujące funkcje oraz protokoły:

- 10/100/1000Mb/s x 24
- 10Gb/s x 4 (2 x 10GbE, 2 x SFP+)
- Magistrala min. 128 Gb/s
- Szybkość przekazywania pakietów ( 64b pakiet ): 95.2 Mpps
- IEEE 802.1Q
- IP VLAN
- MAC VLAN
- Auto Voice VLAN
- Auto Video VLAN
- IEEE 802.1x
- Guest VLAN
- Przydzielanie VLAN na podstawie RADIUS
- RADIUS Accounting
- Access Control Lists (ACLs) L2/L3/L4
- MAC-based ACL
- TCP/UDP-based ACL
- Przypisywanie MAC do portu
- IP Source Guard
- Dynamic ARP inspection
- Ochrona przed DoS
- IEEE 802.3ad
- IEEE 802.3x
- IEEE 802.1D
- IEEE 802.1w
- IEEE 802.1s
- BPDU Guard
- Możliwość łączenia w stos za pomocą SFP+ lub 10GBase-T
- Min. 6 przełączników w stosie
- IGMP Snooping (v1, v2, v3)
- MLD Snooping (v1, v2)
- IGMP Snooping
- Multicast VLAN Registration
- Klient DHCP

- DHCP Snooping
- Tablica ARP min. 512
- Router Discovery (IRDP)
- IEEE 802.3ad
- Manual LAG
- 802.1ab LLDP
- SNMP V1, V2c, V3
- RMON 1,2,3,9
- Listy dostępu L2 MAC, L3 IP oraz L4 ACL
- Ograniczenie pasma na wyjściu
- DiffServ QoS
- IEEE 802.1p COS
- Dst MAC and IP
- IPv4 and v6 DSCP
- Strict Priority
- Zarządzanie IPv6
- SNTP client po UDP port 123
- Port Mirroring
- Port Mirroring wiele do jednego
- Ilość grup multicast 512
- Ilość statycznych tras 32
- Ilość routowalnych VLAN 15
- Ilość ACL min 100 dla MAC lub IP
- Emisja hałasu ANSI-S10.12 max 40dBA
- MTBF min 278 tyś godzin

Zarządzanie za pomocą przeglądarki

**Przełącznik TYP B szt. 6**

Wymaga się aby urządzenie minimalnie obsługiwało następujące funkcje oraz protokoły:

- 10/100/1000Mb/s x 48
- 10Gb/s x 4 (2 x 10GbE, 2 x SFP+)
- Magistrala min. 176Gb/s
- Szybkość przekazywania pakietów ( 64b pakiet ): 95.2 Mpps
- IEEE 802.1Q
- IP VLAN
- MAC VLAN
- Auto Voice VLAN
- Auto Video VLAN
- IEEE 802.1x
- Guest VLAN
- Przydzielanie VLAN na podstawie RADIUS

- RADIUS Accounting
- Access Control Lists (ACLs) L2/L3/L4
- MAC-based ACL
- TCP/UDP-based ACL
- Przypisywanie MAC do portu
- IP Source Guard
- Dynamic ARP inspection
- Ochrona przed DoS
- IEEE 802.3ad
- IEEE 802.3x
- IEEE 802.1D
- IEEE 802.1w
- IEEE 802.1s
- BPDU Guard
- Możliwość łączenia w stos za pomocą SFP+ lub 10GBase-T
- Min. 6 przełączników w stosie
- IGMP Snooping (v1, v2, v3)
- MLD Snooping (v1, v2)
- IGMP Snooping
- Multicast VLAN Registration
- Klient DHCP
- DHCP Snooping
- Tablica ARP min. 512
- Router Discovery (IRDP)
- IEEE 802.3ad
- Manual LAG
- 802.1ab LLDP
- SNMP V1, V2c, V3
- RMON 1,2,3,9
- Listy dostępu L2 MAC, L3 IP oraz L4 ACL
- Ograniczenie pasma na wyjściu
- DiffServ QoS
- IEEE 802.1p COS
- Dst MAC and IP
- IPv4 and v6 DSCP
- Strict Priority
- Zarządzanie IPv6
- SNTP client po UDP port 123
- Port Mirroring
- Port Mirroring wiele do jednego
- Ilość grup multicast 512

- Ilość statycznych tras 32
- Ilość routowalnych VLAN 15
- Ilość ACL min 100 dla MAC lub IP
- Emisja hałasu ANSI-S10.12 max 40dBA
- MTBF min 278 tyś godzin

Zarządzanie za pomocą przeglądarki

**Przełącznik TYP C szt.4**

Wymaga się aby urządzenie minimalnie obsługiwało następujące funkcje oraz protokoły:

- Min. 24 porty( 12 portów SFP+ oraz 12 portów 10GBaseT) niezależne

- Tablica MAC min. 16K
- Tablica ARP/NDP min. 8K
- Bufor 32Mb
- MTBF min. 192 tys. godzin
- Wydajność min. 357 Mp/s
- Przepustowość min. 480 Gb/s
- Port USB
- Port miniUSB
- Port zarządzania Out-of-band;
- Web GUI
- HTTPs
- CLI
- Telnet
- SSH
- SNMP
- MIB RSPAN
- Radius
- TACACS+
- DiffServ
- Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
- IPv4/IPv6 Multicast filtering
- IGMPv3 MLDv2 Snooping
- IGMPv1,v2 Querier
- Auto-VoIP
- Auto-iSCSI
- Policy-based routing (PBR)
- LLDP-MED
- Spanning Tree
- STP

- MTP
- RSTP
- PV(R)STP
- BPDU/STRG Root Guard
- EEE (802.3az)
- GVRP/GMRP
- Q in Q,
- Private VLAN
- DOT1X
- MAB
- Captive Portal
- DHCP Snooping
- Dynamic ARP
- Inspection
- IP Source Guard
- CPU min 800 Mhz
- Min 1GB RAM
- Min 256MB Flash
- Min ilość obsługiwanych VLAN 4K
- DHCP Server min 2K rezerwacji
- sFlow
- Minimalna ilość przełączników w stosie: 8
- Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
- Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
- Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
- Distributed Link Aggregation (LAGs across the stack)
- Ilość interfejsów IP 128
- Double VLAN Tagging (QoQ)
- PIM-DM (Multicast Routing - dense mode)
- PIM-DM (IPv6)
- PIM-SM (Multicast Routing - sparse mode)
- PIM-SM (IPv6)
- RIPv2
- OSPFv2
- RFC 2328
- RFC 1583
- OSPFv2 min. sąsiadów 400
- OSPFv3 min. sąsiadów 400
- OSPFv3 min. sąsiadów na interfejs 100
- DHCPv6 Snooping

- wysyłanie alertów na email
- MMRP

***Gwarancja***

Wymaga się aby urządzenia były objęte gwarancja przez okres 36 miesięcy realizowaną w systemie door-to-door przez serwis producenta.
Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii.
W okresie gwarancji należy zagwarantować bezpłatny dostęp do aktualizacja firmwareu dla dostarczanych urządzeń.

**Kontroler sieci bezprzewodowej 1 komplet**

**Wymagane minimalne parametry techniczne:**

Wymaga się aby oferowany kontroler sieci bezprzewodowej posiadał następujących funkcjonalności:

- Konfiguracja punktów dostępowych
- Zarządzanie politykami bezpieczeństwa
- Zarządzanie politykami QoS
- Dobór obsługiwanych kanałów na punktach dostępowych
- Monitorowanie pasma radiowego pod kątem wykrywania interferencji, pomiaru poziomu utylizacji i szumów w celu dynamicznej optymalizacji ustawień parametrów radiowych
- Zarządzanie mobilnością urządzeń
- Zarządzanie budową sieci kratowej

Gwarancja:

Wymaga się aby urządzenie były objęte gwarancja producenta przez okres 36 miesięcy realizowaną w systemie door-to-door przez serwis producenta.
Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii.

**Acess Point 10 kompletów**

**Wymagane minimalne parametry techniczne:**

- Architektura radiowa i obsługa standardów
  1. Obsługa MIMO 2x2:2
  2. Moduł radiowy 802.11 a/n/ac

- Obsługa zakresów częstotliwości
  1. 2,412 – 2,484 GHz
  2. 5,150 – 5,250 GHz (UNII-1)
  3. 5,250 – 5,350 GHz (UNII-2)
- Zasilanie:
  1. PoE (IEEE 802.3af)
  2. Adapter AC
- Interfejs; 1 x 100/1000 Base-T
- Mechanizmy bezpieczeństwa
  1. WEP, WPA, WPA2-PSK, WPA2-Enterprise (802.1X)
  2. Szyfrowanie TKIP oraz AES
  3. Szyfrowanie IPSec w celu tunelowania danych do koncentratora VPN
  4. Blokowanie ruchu między klientami bezprzewodowymi
- Funkcje ogólne
  1. Konfiguracja min. 6 SSID
  2. Zarządzanie przez interfejs webowy
- Logowanie zdarzeń systemowych

Gwarancja:

Wymaga się aby urządzenie było objęte gwarancja przez okres 36 miesięcy realizowaną w systemie door-to-door przez serwis producenta.
Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii.
W okresie gwarancji należy zagwarantować bezpłatny dostęp do aktualizacja firmwareu dla dostarczanych urządzeń.

**NAS – 1 komplet**

**Wymagane minimalne parametry techniczne:**

- umożliwiająca skonfigurowanie zabezpieczeń RAID: 1,5,6,10
- dyski: minimum 8 x 8TB SAS
- obsługa dysków z prędkościami 3, 6 Gb/s;
- sieć: minimum 4 x 1GbE oraz 1x10GbE
- Gwarancja:
  c. gwarancja producenta na okres 36 miesięcy świadczona na miejscu u klienta

Czas reakcji serwisu - do końca następnego dnia roboczego

d. Oświadczenie, że w przypadku awarii dysk twardy zostaje u Zamawiającego.

**Serwerowy system operacyjny – 3 sztuki**

a. **Oprogramowanie serwerowe**

Wymagane minimalne parametry techniczne:

Do każdego z serwerów musi być dostarczone i zainstalowane oprogramowanie serwerowego systemu operacyjnego. Licencja ma być dostosowana do typu organizacji zamawiającego oraz dostarczonych serwerów. Oprogramowania musi być nowe.

Oprogramowanie musi spełniać minimum następujące funkcjonalności:

Do każdego z serwerów musi być dostarczone oprogramowanie serwerowego systemu operacyjnego
spełniającego minimum następujące funkcjonalności:

1. licencje muszą mieć możliwość instalacji na serwerach wirtualnych
2. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych
3. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe
4. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play)
5. graficzny interfejs użytkownika
6. obsługa systemów wieloprocesorowych
7. obsługa platform sprzętowych x86, x64
8. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu
9. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowego oprogramowania:
   - 9.1. usługi sieciowe DNS i DHCP,
   - 9.2. usługi katalogowe pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z
   - 9.3. dalna dystrybucja oprogramowania na stacje robocze,
   - 9.4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
   - 9.5. PKI (Centrum Certyfikatów, obsługa klucza publicznego i prywatnego),

9.6. szyfrowanie plików i folderów, szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
9.7. możliwość rozłożenia obciążenia serwerów,
9.8. serwis udostępniania stron WWW, serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management),
9.9. wsparcie dla protokołu IP w wersji 6 (IPv6)
10. Możliwość tworzenie serwerów wirtualnych, oprogramowanie wspierające tworzenie serwerów wirtualnych musi spełniać następujące wymagania funkcjonalne:
10.1. warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
10.2. licencja musi umożliwiać jej przenoszenie pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade)
10.3. rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze
10.4. możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-4 wirtualnych kart sieciowych.
10.5. możliwość przydzielania większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji
10.6. możliwość udostępniania maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy
10.7. konsola graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
10.8. możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach
10.9. możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
10.10. możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi
10.11. możliwość integracji z usługami katalogowymi Microsoft Active Directory.
10.12. mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn
10.13. obsługa przełączania ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.
10.14. możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi,

10.15. mechanizm wysokiej dostępności HA, w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym

10.16. funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.

10.17. pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia w razie awarii karty sieciowej

10.18. wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN)

**b. Licencje dostępowe AD**

Licencje do oprogramowania serwerowego dla 90 użytkowników
Do jednego z serwerowych systemów operacyjnych muszą być dostarczone licencje dostępowe do systemu serwerowego w liczbie minimum 90 sztuk.
Zastosowanie licencji dostępowych jest wymagane ze względu na konieczność przeprowadzenia procesu:

- identyfikacji – użytkownik deklaruje swoją tożsamość - w procesie logowania do serwera użytkownik wpisuje nazwę (login);
- uwierzytelniania – serwer stosuje odpowiednią technikę uwierzytelniania w celu weryfikacji zadeklarowanej wcześniej tożsamości - serwer prosi użytkownika o wpisanie hasła (lub wskazanie pliku klucza) i weryfikuje jego zgodność z wcześniej ustawioną wartością;
- autoryzacji – potwierdzenie, czy dany użytkownik jest uprawniony do uzyskania dostępu do żądanego zasobu - serwer weryfikuje uprawnienia zalogowanego użytkownika do konkretnego pliku sprawdzając tablicę dostępu w systemie plików;

Innymi słowy licencje dostępowa są niezbędne by zidentyfikować użytkownika, zweryfikować jego tożsamość i pozwolić uzyskiwać dostęp do przydzielonych mu w uprawnieniach zasobów sieciowych w tym np. katalogów z plikami, dostępu do aplikacji czy urządzeń peryferyjnych (np. drukarek, skanerów).

**Zabezpieczenie styku z Internetem**

Urządzenie winno zapewnić stabilny i bezpieczny sposób komunikacji jednostki z Internetem. W celu niezawodnego i efektywnego połączenia wszystkich użytkowników z systemami centralnymi, urządzenie winno umożliwić zabezpieczenia dostępu z zewnątrz oraz zapewnienia obsługi funkcji bezpieczeństwa – szyfrowania danych, tunelowania oraz uwierzytelniania i autoryzacji użytkownika przy dostępie do sieci VPN.

Wymaga się rozwiązania opartego o dostęp do Internetu z wykorzystaniem urządzeń wielofunkcyjnej zapory sieciowej np. UTM, Zapora będzie obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych:

- firewall, IPS, antywirus, kontrola treści (WWW i aplikacji),
- poufność danych – IPSec VPN oraz SSL VPN, z uwzględnieniem identyfikacji poszczególnych użytkowników lub grup użytkowników.

Parametry wydajnościowe zainstalowanego urządzenia do ochrony styku z Internetem powinny mieć wydajność nie mniejsza niż 200 Mb/s i obsługiwać nie mniej niż 100 użytkowników.

**a. Klaster HA złożony z 2 sztuk urządzeń typu 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. Powinna istnieć możliwość dedykowania co najmniej 8 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. System musi zostać dostarczony w postaci klastra wysokiej dostępności (HA) – dwa urządzenia.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

- 18 portami Gigabit Ethernet RJ-45.
- 4 gniazdami SFP 1 Gbps.
- 2 gniazdami SFP+ 10 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1,5 mln jednoczesnych połączeń oraz 56.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.2 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 11.5 Gbps.
6. 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 2,6 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - 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, IMAP.
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.
12. Analiza ruchu szyfrowanego protokołem SSH,

<u>Polityki, Firewall</u>

1. Polityka Firewall musi uwzględniać 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:

- 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.

<u>Połączenia VPN</u>

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.

<u>Routing i obsługa łączy WAN</u>

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- Routingu statycznego.
- Policy Based Routingu.

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

2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

<u>Zarządzanie pasmem</u>

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.

<u>Kontrola Antywirusowa</u>

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).

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna 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 avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

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

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

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. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. System musi mieć możliwość logowania 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 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.

Certyfikacje

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA lub NSS Labs dla funkcji IPS.
- ICSA dla funkcji IPsec VPN oraz SSL VPN

Serwisy i licencje

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

a) Firmware, Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres co najmniej 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać wsparcie techniczne w trybie od pon. do pt., od 8:00 do 16:00 Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać odpowiedni

certyfikat w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- podmiot serwisujący posiadający odpowiednie uprawnienia i kwalifikacje.

**b. System Centralnego Logowania i Raportowania Systemów**

Wymagania Ogólne

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

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

Interfejsy, Dysk

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

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 2 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

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: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

- Malware.
- Aplikacje sieciowe.
- Email.

- IPS.
- Traffic.
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

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

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

2. System musi umożliwiać zdefiniowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Gwarancja oraz wsparcie

System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz przez okres 36 miesięcy wsparciem technicznym co najmniej w trybie 8x5.

***Pozostałe prace oraz materiały związane z zamówieniem***

W ramach projektu należy dostarczyć, zamontować i skonfigurować urządzenie UTM oraz system zbierania logów.
Dostarczone urządzenia należy zamontować w wyznaczonych przez Zamawiającego miejscach zgodnie z punktem 11 „Pozostałe prace oraz materiały związane z zamówieniem" połączyć z infrastrukturą realizowaną w projekcie oraz odpowiednio zasilić.
Wykonawca dokona rozeznania potrzeb klienta i zaproponuje sposób połączenia dostarczonych urządzeń oraz propozycję wstępnej konfiguracji zwracając szczególną uwagę na ochronę sieci wewnętrznej.

Po pozytywnej akceptacji sposobu wdrożenia przez Zamawiającego należy wykonać wszelkie czynności w celu ich realizacji.
Wszelkie prace konfiguracyjne maja być wykonane w siedzibie Zamawiającego w obecności przedstawiciela Zamawiającego
Przeprowadzenie instruktażu na podstawie w/w elementów dla całości instalacji od ustawień domyślnych do finalnej konfiguracji zawierającej wszystkie wymagane funkcjonalności oraz monitorowanie podstawowych parametrów pracy przełącznika.
Dostarczenie wszelkich niezbędnych materiałów koniecznych do zestawienia połączeń pomiędzy dostarczanymi urządzeniami a realizowaną infrastrukturą są w zakresie Wykonawcy.

W ofercie wymagane jest podanie modelu, symbolu oraz producenta proponowanego sprzętu.

**Szkolenia**

W ramach realizacji zamówienia Wykonawca przeprowadzi cykl szkoleń dla wyznaczonego przez Zamawiającego personelu.

Wykonawca w zakresie dostarczanego środowiska serwerowo-macierzowego wraz z systemem operacyjnym przeprowadzi szkolenia:

1. Konfiguracji i zarządzania systemem serwerowym dla 2 osób
2. Konfiguracji i zarządzania kopii bezpieczeństwa dla 2 osób
3. Konfiguracji i zarządzania bezpieczeństwem informacji dla 2 osób

Na etapie wdrożenia strony ustalą szczegółowy porządek i podział szkoleń z uwzględnieniem wymagań zawartych w niniejszym rozdziale, które przyjęte zostaną w Planie szkoleń.

**Szkolenie dla administratorów z zakresu:**

- **konfiguracji i zarządzania systemem serwerowym**
- **konfiguracji i zarządzania kopią bezpieczeństwa**

Wymagania:

- szkolenie ma się odnosić do dostarczonego środowiska serwerowo-macierzowego
- prezentacja dostarczonych produktów;
- omówienie architektury wdrożonego środowiska;
- przekazanie wiedzy niezbędnej do poprawnego administrowania dostarczonym środowiskiem serwerowo-macierzowym
- przekazanie wiedzy w zakresie niezbędnych analiz, sprawozdań i raportów
- omówienie zasad i procedur administrowania w tym konfiguracji urządzeń i środowiska, wirtualizacji oraz monitorowania środowiska
- omówienie zasad i procedur niezbędnych do wykonywania i zarządzania kopią bezpieczeństwa

**Szkolenie dla administratorów z zakresu:**

- **konfiguracji i zarządzania bezpieczeństwem informacji**

Wymagania:

- szkolenie ma się odnosić do dostarczonego systemu informatycznego
- przekazanie wiedzy niezbędnej do poprawnego administrowania dostarczonym systemem informatycznym
- przekazanie wiedzy w zakresie niezbędnych analiz, sprawozdań i raportów
- prezentacja dostarczonego systemu; zapoznanie z systemem bezpieczeństwa; omówienie konfiguracji systemu bezpieczeństwa;
- przedstawienie zasad i procedur administrowania i monitorowania pracy systemu bezpieczeństwa.

**Ogólne warunki szkoleń**
**Obowiązkiem Wykonawcy będzie:**

1. przeprowadzić szkolenia z wdrażanych rozwiązań
2. przygotować infrastrukturę szkoleniową w udostępnionych salach szkoleniowych ( minimum: rzutnik i ekran, a w razie potrzeby switch, serwer szkoleniowy, konfiguracja stanowisk),
3. uzyskać akceptację Zamawiającego co do zakresu i formy materiałów szkoleniowych, przed udostepnieniem materiałów szkoleniowych uczestnikom.
4. przeprowadzić szkolenia na podstawie zaakceptowanego przez Zamawiającego harmonogramu szkoleń, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 7 dni przed rozpoczęciem szkolenia.
5. zapewnić każdemu uczestnikowi materiały szkoleniowe,
6. zapewnić obsługę cateringową (tzw. susz konferencyjny, woda, kawa, herbata),
7. zapewnić w trakcie szkoleń oraz w materiałach szkoleniowych, oznakowanie zgodne z wytycznymi IZ RPO WŁ na lata 2014-2020 informujące o współfinansowaniu projektu z UE,
8. sporządzić dokumentację fotograficzną i papierową z przeprowadzonych szkoleń
9. wszystkim uczestnikom szkolenia po ukończeniu szkolenia wystawić zaświadczenia
10. zapewnienie kadry trenerskiej posiadającej wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.

**Szkolenia będą musiały spełniać minimum następujących wymagania :**

1. zajęcia powinny odbywać się od poniedziałku do piątku w godzinach od godz. 8 do 16,
2. zajęcia nie będą mogły trwać dłużej niż 6 godzin lekcyjnych dziennie.
3. szkolenia odbywać się będą w siedzibie/placówkach Zamawiającego. Zamawiający udostępni Wykonawcy salę szkoleniową.

Zajęcia muszą być prowadzone metodą warsztatów aktywizującą uczestników szkoleń, przy

czym każda osoba powinna mieć do dyspozycji osobne stanowisko komputerowe.

**Odbiór produktu typu szkolenia**

Produkt szkolenia będzie odbierany każdorazowo z przekazanych do akceptacji Zamawiającego materiałów szkoleniowych oraz listy obecności uczestników szkolenia. Pracownicy Zamawiającego mają obowiązek podpisania listy obecności na szkoleniu. Na podstawie materiałów szkoleniowych i listy obecności podpisywany jest przez strony protokół odbioru szkolenia z każdego zakresu.

**Pozostałe prace oraz materiały związane z zamówieniem**

3. W ramach tego zadania zostanie zrealizowana dostawa, instalacja i konfiguracja zamawianych urządzeń.
4. Miejsca lokalizacji przedmiotu zamówienia:
   - Złotnickiego 25 budynek A , Zduńska Wola – PD_1
   - Złotnickiego 25 budynek B , Zduńska Wola – PD_2
   - Królewska 10, Zduńska Wola – PD_3
   - Żeromskiego 10a, Zduńska Wola – PD_4
5. Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa zamówionego sprzętu do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone powyżej oraz ich zamontowanie wyżej wymienionych przez Zamawiającego miejscach, a także wykonanie wszystkich niezbędnych usług instalacyjnych i konfiguracyjnych ( w tym: zainstalowanie serwerowego systemu operacyjnego, sterowników, dysków, skonfigurowanie macierzy, skonfigurowanie NAS , montaż w szafie rack, skonfigurowanie RAID , konfiguracja kontrolera sieci bezprzewodowej, zamontowanie i konfiguracja Access Pointów, konfiguracja bezpiecznego styku z internetem, wpięcie do istniejącej sieci informatycznej Zamawiającego, konfiguracja do 15 VLAN, wstępna konfiguracja AD lub usługi równoważnej), zgodnie ze sztuką, zaleceniami producenta, wskazaniami Zamawiającego oraz najlepszymi praktykami koniecznych by dostarczone urządzenie funkcjonowało poprawnie w środowisku informatycznym Zamawiającego i zapewniały bezawaryjną i bezpieczną pracę użytkownikom końcowym.
6. Wszystkie dostarczane urządzenia (poza Access Point) Wykonawca zamontuje w dedykowanych szafach rack rozlokowanych w 4 budynkach PD_1, PD_2, PD_3, PD_4 na terenie Zduńskiej Woli. (Zamawiający preferuje urządzenia w obudowach typu rack, Zamawiający dysponuje ograniczonym miejscem w szafach rack). Odległość pomiędzy poszczególnymi lokalizacjami nie przekracza 750m.
   - PD_1 1xTYP-A 2xTYP-B 2xTYP-C , NAS

- PD_2 1xTYP-B
- PD_3 2xTYP-B 2xTYP-C , 3 serwery, macierz, UTM
- PD_4 1xTYP-B

7. Wszystkie budynki połączone są światłowodem jednomodowym.
8. Wykonawca zainstaluje i skonfiguruje Access Pointy we wszystkich lokalizacjach – PD_1, PD_2, PD_3, PD_4.
9. Wszystkie dostarczone urządzenia należy odpowiednio połączyć i podłączyć do infrastruktury Zamawiającego oraz odpowiednio zasilić z dostępnej instalacji elektrycznej.
10. Dostarczenie wszelkich niezbędnych materiałów koniecznych do zestawienia połączeń pomiędzy dostarczanymi urządzeniami oraz infrastrukturą Zamawiającego są w zakresie Wykonawcy.
11. Sposób połączenia zakupionego sprzętu oraz jego konfiguracji winien być wykonany z uwzględnieniem odporności na awarię oraz zapewnieniem dużej wydajności i integralności danych.
12. Dla prawidłowego połączenia dostarczonych urządzeń oraz wpięcia ich w istniejącą infrastrukturą Zamawiającego wymaga się zastosowania połączeń redundantnych opartych o moduły SFP+ działające na światłowodzie jednomodowym w technologii full duplex kompatybilne z dostarczonymi sprzętem. Dopuszcza się zestawienie połączeń opartych o porty 10GbE tam gdzie będzie zbyt mała ilość SFP+. Należy zestawić połączenia tak by zapewnić jak najbardziej stabilny i szybki przepływ danych.
13. Wszelkie prace konfiguracyjne maja być wykonane w siedzibie Zamawiającego w obecności przedstawiciela Zamawiającego.
14. Wykonawca przy współpracy z Zamawiającym dokona rozeznania potrzeb Zamawiającego i zaproponuje sposób połączenia oraz konfiguracji dostarczonego sprzętu i oprogramowania w środowisku i z wykorzystaniem infrastruktury Zamawiającego gwarantującego jego odpowiednią pracę i odporność na awarię.
15. Wykonawca zobowiązany jest do przeprowadzenia instruktażu na podstawie dostarczonego, zainstalowanego i skonfigurowanego rozwiązania dla całości instalacji od ustawień domyślnych do finalnej konfiguracji zawierającej wszystkie wymagane funkcjonalności odpowiednie do środowiska informatycznego Zamawiającego.
16. Wymaga się utrzymania wsparcia technicznego przez osoby posiadające odpowiednie uprawnienia i kwalifikacje w okresie gwarancji przez 5 dni w tygodniu (od poniedziałku do piątku) w godzinach od 8:00 do 16:00