# **Zamówienie obejmuje:**

* 1. Dostawę urządzeń sieciowych zgodnie z opisem w pkt 4.:
     1. Przełącznik brzegowy – 2 sztuki;
     2. Kontroler urządzeń dostępowych i system bezpieczeństwa – 2 sztuki;
     3. Przełącznik główny – 2 sztuki;
     4. Przełącznik dostępowy – 20 sztuk;
     5. Moduły optyczne – łącznie wszystkich 214 sztuk.

# Dostawę oprogramowania do ww. urządzeń sieciowych, zgodnie z opisem w pkt 5.:

* + 1. Centralny system do zarządzania;
    2. Centralny system kolekcji i korelacji logów.

# Wdrożenie urządzeń sieciowych i oprogramowania, zgodnie z opisem w pkt 6.

# Zapewnienie 3-letniego pakietu gwarancyjnego i licencyjnego, zgodnie z opisem w pkt 7.

# Usługi wsparcia Wykonawcy w wymiarze maksymalnie do 600 godzin w okresie trwania umowy, zgodnie z opisem w pkt 8.

# **Wymagania ogólne do zamówienia:**

* 1. W ramach postępowania wymagane jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie rządzeń wraz ze Wsparciem Producenta oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa i posiadaną infrastrukturą Zamawiającego.
  2. Zamawiający jest w posiadaniu rozwiązania FortiGate pracującego w klastrze, punktów dostępu WLAN Forti Aacces Point oraz i Forti Analyzer.
  3. Poprzez rozbudowę istniejącego systemu, celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową oraz dostarczenie przełączników oraz innych elementów funkcjonalnych, współpracujących z istniejącym u Zmawiającego rozwiązaniem Fortigate, systemem FortiAnalyzer oraz Access Point Fortinet.

# **Wymagania ogólne dotyczące urządzeń sieciowych i oprogramowania do zarządzania oraz kolekcji i korelacji logów:**

* 1. Dostarczone urządzenia muszą być sprawne technicznie, fabrycznie nowe i nieużywane wcześniej w żadnych innych projektach.
  2. Nie dopuszcza się zaoferowania urządzeń typu „refubrished” tj. zwróconych do producenta i później odsprzedawanych ponownie przez producenta.
  3. Oferowany sprzęt i systemy muszą pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski.
  4. Urządzenia będą dopuszczone do sprzedaży i eksploatacji w Polsce.
  5. Oferowany sprzęt i systemy muszą być objęte serwisem producenta lub serwisem autoryzowanym przez producenta zaoferowanego sprzętu.
  6. Wykonawca przedłoży na żądanie Zamawiającego oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

# **Dostawa urządzeń sieciowych:**

# Szczegółowe wymagania ilościowe urządzeń sieciowych.

|  |  |  |  |
| --- | --- | --- | --- |
| LP | Urządzenie | Ilość | Uwagi |
|  | „przełącznik brzegowy” | 2 | Dodatkowo wyposażony w kompatybilne wkładki zgodnie z ilościowymi wymaganiami. |
|  | „Kontroler urządzeń dostępowych i system bezpieczeństwa” | 2 | Dodatkowo wyposażony w kompatybilne wkładki zgodnie z ilościowymi wymaganiami. |
|  | „przełącznik główny” | 2 | Dodatkowo wyposażony w kompatybilne wkładki zgodnie z ilościowymi wymaganiami. |
|  | „przełącznik dostępowy” | 20 | Dodatkowo wyposażony w kompatybilne wkładki zgodnie z ilościowymi wymaganiami. |
|  | System zarządzania | 1 | Maszyna wirtualna |
|  | System kolekcji i korelacji logów | 1 | Maszyna wirtualna |
|  | Moduł optyczny typu LC SINGLE RATE BiDi 10GE SFP+, short range,  przeznaczony do realizacji połączeń na jednym włóknie jednomodowym. | 198 | Połączenia lokalne LAN |
|  | Moduł optyczny typu LC SINGLE RATE BiDi 100GE QSFP28 SFP+, long range,  przeznaczony do realizacji połączeń na jednym włóknie jednomodowym. | 4 | Połączenie pomiędzy serwerowniami w osobnych budynkach |
|  | Moduł optyczny typu LC SINGLE RATE BiDi 100GE QSFP28 SFP+, short range, przeznaczony do realizacji połączeń na jednym włóknie jednomodowym. | 12 | Połączenia lokalne LAN |

* 1. **Wymagania dla urządzeń typu „przełącznik brzegowy” – 2 sztuki.**

Wymagania dla przełączników sieciowych łączących nową lokalizację z obecną lokalizacją Zamawiającego. 

* + 1. Parametry fizyczne platformy
       1. Wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U.
       2. Redundantne zasilanie 230V, maksymalny pobór mocy 250W.
       3. Zakresy temperatury pracy – 0-40’C.
       4. MTBF > 10lat.
    2. Interfejsy sieciowe – wymagania minimalne
       1. Co najmniej 24 porty 10 GE SFP+ (z obsługą wkładek 1GE).
       2. Co najmniej 2 porty 100 GE/40 GE QSFP28/QSFP+.
    3. Zarządzanie
       1. Dedykowany interfejs do zarządzania GE – RJ-45.
       2. Port konsoli szeregowej.
       3. Zarządzanie przez konsolę szeregową, interfejs tekstowy (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę.
       4. Zarządzanie poprzez centralny system zarządzania pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniami typu kontroler urządzeń dostępowych i system bezpieczeństwa.
       5. Centralny system zarządzania musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.
       6. Centralny system zarządzania musi umożliwiać aktualizację oprogramowania zarządzanych przełączników.
       7. Z poziomu centralnego systemu zarządzania musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).
    4. Parametry wydajnościowe
       1. Przepustowość urządzenia - min. 850 Gbps, min. 1300 Mpps.
       2. Możliwość zapamiętania co najmniej 64.000 adresów MAC.
       3. Opóźnienie - poniżej 1 mikrosekund.
       4. Bufor pakietów: min. 8 MB.
       5. Pamięć DRAM: min. 8 GB.
    5. Wymagane funkcje
       1. Automatyczna negocjacja prędkości i duplexu dla połączeń
       2. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree), ilość instancji min 15.
       3. Agregacja portów zgodna z 802.3ad, ilość grup min. 24, ilość portów w grupie: min. 24.
       4. Obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
       5. Możliwość wykonywania routingu statycznego.
       6. Możliwość wykonywania routingu dynamicznego (OSPFv2, RIPv2) – jeżeli funkcjonalność wymaga dodatkowej licencji, to nie jest ona wymagana do dostarczenia.
       7. Wsparcie dla ECMP (Equal-cost multi-path routing) oraz BFD (Bidirectional Forwarding Detection).
       8. Funkcjonalność DHCP Relay, DHCP Snooping, Dynamic ARP Inspection, IGMP Snooping.
       9. Port-mirroring.
       10. Obsługa MAC Sec (IEEE 802.1ae MAC Security) również na portach typu trunk.
       11. Obsługa sFlow.
       12. Obsługa list kontrolnych ACL, min. 3000 wpisów.
       13. Wsparcie dla protokołu wysokiej dostępności MCLAG (multi-chassis link aggregation).
       14. Kontrola dostępu na poziomie portu w oparciu o standard 802.1x (port oraz MAC-based), możliwość uwierzytelniania w oparciu o bazę Radius.
       15. Zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS.
       16. Wsparcie dla SNTP, LLDP (w trybie odbioru).
       17. Wsparcie dla SNMP w wersjach 1 – 3.
       18. Możliwość zarządzania przez interfejs graficzny i tekstowy.
       19. Możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI
       20. Wsparcie dla HTTP REST API dla konfiguracji i monitoringu.
       21. Integracja z systemem spełniającym funkcję kontrolera urządzeń dostępowych i systemem bezpieczeństwa polegająca na przekierowaniu całego ruchu w obrębie tego samego VLAN-u przez urządzenie bezpieczeństwa i filtracja tego ruchu z wykorzystaniem mechanizmów bezpieczeństwa, np. IPS, AV.
    6. Funkcje urządzenia przy integracji z kontrolerem urządzeń dostępowych i systemem bezpieczeństwa
       1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny czyli oferowany w ramach tego postępowania kontroler urządzeń dostępowych i system bezpieczeństwa. Zakres integracji musi być tożsamy i wymienny z posiadanymi przez Zamawiającego firewall’ami.
       2. Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
          1. Centralne zarządzanie konfiguracją urządzenia.
          2. Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania.
          3. Centralne zarządzanie sieciami VLAN.
          4. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u.
          5. Możliwość rozpoznawania urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki itp., w oparciu o bazę posiadaną i uaktualnianą przez producenta elementu nadrzędnego.
          6. Przenoszenie zidentyfikowanych urządzeń do właściwych stref w przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, np. element nadrzędny może przenieść urządzenie końcowe do strefy odizolowanej (kwarantanny) w przypadku wykrycia anomalii.
          7. Integrację z podstawowym systemem kontroli dostępu znajdującym się na elemencie nadrzędnym. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: adresu mac, nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego, grupy użytkowników (w tym również możliwość integracji z zewnętrznym system LDAP – mapowanie grup).
          8. Przesyłanie logów na zewnętrzny serwer syslog.
          9. Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników w dostępie do sieci.
          10. Obsługa białych i czarnych list adresów MAC.
          11. Wykrywanie aplikacji komunikujących się w sieci.
    7. Moduły optyczne

Wraz z przełącznikami należy dostarczyć następujące moduły sieciowe światłowodowe. Ilość oraz typ została podana w tabeli zbiorczej. Moduły muszą być oficjalnie wspierane przez producenta urządzeń.

* 1. **Wymagania dla urządzeń typu** **kontroler urządzeń dostępowych i system bezpieczeństwa (2 sztuk Firewalli)**
     1. Wymagania Ogólne
        1. Urządzenia muszą być tego samego modelu, o tej samej konfiguracji sprzętowej, objęte identycznymi pakietami gwarancyjnymi i licencyjnymi.
        2. Urządzenia będą podłączone w klaster wysokiej dostępności i niezawodności (Active-Active lub Active-Passive).
        3. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa. 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.
        4. System realizujący funkcję kontrolera urządzeń dostępowych i system bezpieczeństwa wewnętrznego musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
        5. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 10 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, IPS. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.
        6. System musi wspierać IPv4 oraz IPv6 w zakresie: firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.
     2. Redundancja, monitoring i wykrywanie awarii
        1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach musi istnieć funkcja synchronizacji sesji firewall.
        2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
        3. Monitoring stanu realizowanych połączeń VPN.
        4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Musi istnieć możliwość tworzenia interfejsów redundantnych.
     3. Interfejsy, zasilanie
        1. System realizujący funkcję Firewall musi dysponować minimum:
           1. 2 portami Gigabit Ethernet RJ-45 do zarządzania.
           2. 16 portami GE RJ45
           3. 8 gniazdami GE SFP
           4. 12 gniazdami 25GE SFP28/ 10GE SFP+/ GE SFP
           5. 4 gniazdami 100GE QSFP28
        2. System musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB oraz instalacji oprogramowania z klucza USB.
        3. W ramach systemu Firewall musi być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
        4. System musi być wyposażony w redundantne zasilanie AC.
     4. Parametry wydajnościowe
        1. W zakresie Firewall’a obsługa nie mniej niż 12 mln jednoczesnych połączeń oraz 750 000 nowych połączeń na sekundę.
        2. Przepustowość Stateful Firewall: nie mniej niż 190 Gbps dla pakietów o rozmiarze 1518B.
        3. Przepustowość Stateful Firewall: nie mniej niż 135 Gbps dla pakietów wielkości 64B.
        4. Wydajność szyfrowania VPN IPSec dla pakietów wielkości 512B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 30 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 zbliżonej do typowych środowisk sieciowych klasy komercyjnej - minimum 20Gbps.
        6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 11Gbps.
     5. 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. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
      3. Ochrona przed atakami - Intrusion Prevention System.
      4. Analiza ruchu szyfrowanego protokołem SSL.
      5. Analiza ruchu szyfrowanego protokołem SSH.
      6. Zarządzanie pasmem (QoS, Traffic shaping).
      7. 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 dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
    1. Polityki, Firewall
       1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, reakcje zabezpieczeń na zdarzenie, rejestrowanie zdarzeń.
       2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
          1. Translację jeden do jeden oraz jeden do wielu.
          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.
       5. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
       6. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
          1. Amazon Web Services (AWS).
          2. Microsoft Azure.
          3. OpenStack.
          4. VMware NSX.
          5. Kubernetes.
    2. Połączenia VPN
       1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
          1. Wsparcie dla IKE v1 oraz v2.
          2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
          3. Obsługa protokołu Diffie-Hellman grup 19, 20.
          4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
          5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
          6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
          7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
          8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
          9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
          10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
          11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
          12. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
       2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
          1. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
          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.
    3. 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, oznaczeń Type of Service w nagłówkach IP).
      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.
    1. 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)
       3. Każde nowe połączenie musi być kierowane do łącza zależnie od aktualnej kondycji łączy badanej w oparciu o parametry takie jak: opóźnienie, jitter, straty pakietów.
    2. 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.
    3. 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. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
       4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
       5. System zapewnia 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).
       7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
       8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
       9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
    4. Uwierzytelnianie użytkowników w ramach sesji
       1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
          1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
          2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
          3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
       2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
       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.
    5. 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. Musi być możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego 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.
       6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
       7. Element systemu realizujący funkcję Firewall 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.
       10. Firewall musi być zarządzany w pełni poprzez system zarządzania będący częścią zapytania.
    6. Integracja z urządzeniami dostępowymi
       1. System musi zarządzać punktami dostępowymi WiFi Fortinet AP posiadanymi przez Zamawiającego z wykorzystaniem protokołu CAPWAP.
       2. Wymaga się aby zarządzaniem punktami dostępowymi można było objąć docelowo 100 punktów dostępowymi wifi.
       3. Minimalny zakres zarządzania z systemu kontroler urządzeń dostępowych i system bezpieczeństwa
          1. Sieci SSID, VLAN muszą być widziane jako interfejsy tego samego systemu.
          2. Wszystkie czynności konfiguracyjne muszą być realizowane z poziomu interfejsu zarządzania tego systemu
          3. Musi być możliwa ręczna i automatyczna aktualizacja oprogramowania AP (firmware)
          4. Musi być widoczny status zarządzanych AP
          5. Musi być widoczny graficznie status podłączonych klientów WiFi (nazwa, siła sygnału, zastosowany standard połączenia, wykorzystana częstotliwość, nazwa użytkownika, itp.)
          6. kontroler urządzeń dostępowych i system bezpieczeństwa musi spełniać funkcje kontrolera WiFi dla podłączonych AP.
          7. Musi być logowanie sieci WiFi zintegrowane z logowaniem tego systemu
          8. Musi być możliwość definicji i konfiguracji profili radiowych dla każdego AP (zakresy częstotliwości, standard pracy, parametry radiowe)
    7. Logowanie
       1. Elementy systemu bezpieczeństwa realizują logowanie do systemu kolekcji i korelacji logów.
       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.
    8. Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

* + 1. Serwisy i licencje

W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów w tym także wykrywanie ataków sieciowych (IPS), przez okres minimum 36 miesięcy.

* 1. **Wymagania dla urządzeń typu „przełącznik główny”**
     1. Parametry fizyczne platformy
        1. Wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U.
        2. Redundantne zasilanie 230V, maksymalny pobór mocy 200W.
        3. MTBF > 10lat.
     2. Interfejsy sieciowe – wymagania minimalne
        1. 48 portów 25GE, SFP28.
        2. 8 portów 100GE, QSFP28.
        3. 2 porty 10 GE SFP+.
     3. Zarządzanie
        1. Dedykowany interfejs do zarządzania GE – RJ-45.
        2. Port konsoli szeregowej.
        3. Zarządzanie przez konsolę szeregową, interfejs tekstowy (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę.
        4. Możliwość zarządzania poprzez centralny system zarządzania pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniem typu kontroler urządzeń dostępowych i systemem bezpieczeństwa.
        5. Centralny system zarządzania musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.
        6. Centralny system zarządzania musi umożliwiać aktualizację oprogramowania zarządzanych przełączników.
        7. Z poziomu centralnego systemu zarządzania musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).
     4. Parametry wydajnościowe
        1. Przepustowość urządzenia - min. 4000 Gbps, min. 4000 Mpps.
        2. Możliwość zapamiętania co najmniej 96000 adresów MAC.
        3. Opóźnienie  - poniżej 1 mikrosekundy.
        4. Bufor pakietów: min. 32 MB.
        5. Pamięć DRAM: min. 8 GB.
        6. Pamięć FLASH: min. 8 GB.
        7. Dysk SSD: min 32GB.
     5. Wymagane funkcje
        1. Automatyczna negocjacji prędkości i duplexu dla połączeń.
        2. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree), ilość instancji min 15.
        3. Agregacja portów zgodna z 802.3ad, ilość grup min. 24, ilość portów w grupie: min. 24.
        4. Obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
        5. Możliwość wykonywania routingu statycznego
        6. Możliwość wykonywania routingu dynamicznego (OSPFv2, RIPv2) – jeżeli funkcjonalność wymaga dodatkowej licencji, to nie jest ona wymagana do dostarczenia
        7. Wsparcie dla ECMP (Equal-cost multi-path routing) oraz BFD (Bidirectional Forwarding Detection)
        8. Funkcjonalność DHCP Relay, DHCP Snooping, Dynamic ARP Inspection, IGMP Snooping.
        9. Port-mirroring.
        10. Obsługa MAC Sec (IEEE 802.1ae MAC Security) również na portach typu trunk
        11. Obsługa sFlow.
        12. Obsługa list kontrolnych ACL, min. 3000 wpisów
        13. Wsparcie dla protokołu wysokiej dostępności MCLAG (multi-chassis link aggregation).
        14. Kontrola dostępu na poziomie portu w oparciu o standard 802.1x (port oraz MAC-based), możliwość uwierzytelniania w oparciu o bazę Radius.
        15. Zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS.
        16. Wsparcie dla SNTP, LLDP (w trybie odbioru).
        17. Wsparcie dla SNMP w wersjach 1 – 3.
        18. Zarządzania przez interfejs graficzny i tekstowy.
        19. Aktualizacja oprogramowania przez TFTP/FTP oraz za pomocą GUI.
        20. Wsparcie dla HTTP REST API dla konfiguracji i monitoringu.
        21. Integracja z systemem spełniającym funkcję kontrolera urządzeń dostępowych i systemem bezpieczeństwa polegająca na przekierowaniu całego ruchu w obrębie tego samego VLAN-u przez urządzenie bezpieczeństwa i filtracja tego ruchu z wykorzystaniem mechanizmów bezpieczeństwa, np. IPS, AV.
     6. Funkcje urządzenia przy integracji z kontrolerem urządzeń dostępowych i systemem bezpieczeństwa.
        1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny czyli oferowany w ramach tego postępowania kontroler urządzeń dostępowych i system bezpieczeństwa. Zakres integracji musi być tożsamy i wymienny z posiadanymi przez Zamawiającego firewall’ami.
        2. Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
           1. Centralne zarządzanie konfiguracją urządzenia.
           2. Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania.
           3. Centralne zarządzanie sieciami VLAN.
           4. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u.
           5. Możliwość rozpoznawania urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki itp., w oparciu o bazę posiadaną i uaktualnianą przez producenta elementu nadrzędnego.
           6. Przenoszenie zidentyfikowanych urządzeń do właściwych stref w przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, np. element nadrzędny może przenieść urządzenie końcowe do strefy odizolowanej (kwarantanny) w przypadku wykrycia anomalii.
           7. Integrację z podstawowym systemem kontroli dostępu znajdującym się na elemencie nadrzędnym. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: adresu mac, nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego, systemu operacyjnego, grupy użytkowników (w tym również możliwość integracji z zewnętrznym system LDAP – mapowanie grup).
           8. Przesyłanie logów na zewnętrzny serwer syslog.
     7. Moduły optyczne

Wraz z przełącznikami należy dostarczyć następujące moduły sieciowe światłowodowe. Ilość oraz typ została podana w tabeli zbiorczej. Moduły muszą być oficjalnie wspierane przez producenta urządzeń.

* 1. **Wymagania dla urządzeń typu „przełącznik dostępowy”.**
     1. Parametry fizyczne platformy:
        1. wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U.
        2. Redundantne zasilanie 230V, maksymalny pobór mocy 50W.
        3. MTBF > 10lat.
     2. Interfejsy sieciowe – wymagania minimalne:
        1. 48 porty GE, RJ-45.
        2. porty 10 GE SFP+ (z obsługą wkładek 1GE).
     3. Zarządzanie.
        1. Dedykowany interfejs do zarządzania GE – RJ-45.
        2. Port konsoli szeregowej.
        3. Zarządzanie przez konsolę szeregową, interfejs tekstowy (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę
        4. Możliwość zarządzania poprzez centralny system zarządzania pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniem typu kontroler urządzeń dostępowych i systemem bezpieczeństwa.
        5. Centralny system zarządzania musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.
        6. Centralny system zarządzania musi umożliwiać aktualizację oprogramowania zarządzanych przełączników.
        7. Z poziomu centralnego systemu zarządzania musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).
     4. Parametry wydajnościowe
        1. Przepustowość urządzenia - min. 175 Gbps, min. 260 Mpps.
        2. Możliwość zapamiętania co najmniej 32000 adresów MAC
        3. Opóźnienie  - poniżej 1 mikrosekundy.
        4. Bufor pakietów: min. 4 MB.
        5. Pamięć DRAM: min. 1 GB.
        6. Pamięć FLASH: min. 256 MB.
     5. Wymagane funkcje
        1. Automatycznej negocjacji prędkości i duplexu dla połączeń
        2. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
        3. Agregacji portów zgodna z 802.3ad, ilość grup min. 26, ilość portów w grupie: min. 8.
        4. Obsługa co najmniej 4000 VLANów, zgodna z 802.1Q.
        5. Możliwość wykonywania routingu statycznego.
        6. Możliwość wykonywania routingu dynamicznego (OSPFv2, RIPv2) – jeżeli funkcjonalność wymaga dodatkowej licencji, to nie jest ona wymagana do dostarczenia.
        7. Funkcjonalność DHCP Relay, DHCP Snooping, Dynamic ARP Inspection, IGMP Snooping.
        8. Port-mirroring.
        9. Obsługa sFlow.
        10. Obsługa list kontrolnych ACL.
        11. Wsparcie dla protokołu wysokiej dostępności MCLAG (multi-chassis link aggregation).
        12. kontrola dostępu na poziomie portu  w oparciu o standard 802.1x (port oraz MAC-based), możliwość uwierzytelniania w oparciu o bazę Radius.
        13. Zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS.
        14. Wsparcie dla SNTP oraz LLDP (w trybie odbioru).
        15. Wsparcie dla SNMP w wersjach 1 – 3.
        16. Zarządzanie przez interfejs graficzny i tekstowy.
        17. Aktualizacja oprogramowania przez TFTP/FTP oraz za pomocą GUI.
        18. Wsparcie dla HTTP REST API dla konfiguracji i monitoringu.
        19. Integracja z systemem spełniającym funkcję kontrolera urządzeń dostępowych i systemem bezpieczeństwa polegająca na przekierowaniu całego ruchu w obrębie tego samego VLAN-u przez urządzenie bezpieczeństwa i filtracja tego ruchu z wykorzystaniem mechanizmów bezpieczeństwa, np. IPS, AV.
     6. Funkcje urządzenia przy integracji z kontrolerem urządzeń dostępowych i systemem bezpieczeństwa.
        1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny czyli oferowany w ramach tego postępowania systemem kontrolera urządzeń dostępowych i system bezpieczeństwa. Zakres integracji musi być tożsamy i wymienny z posiadanymi przez Zamawiającego firewall’ami.
        2. Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
           1. Centralne zarządzanie konfiguracją urządzenia.
           2. Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania.
           3. Centralne zarządzanie sieciami VLAN.
           4. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u.
           5. Możliwość rozpoznawania urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki itp., w oparciu o bazę posiadaną i uaktualnianą przez producenta elementu nadrzędnego.
           6. Przenoszenie zidentyfikowanych urządzeń do właściwych stref w przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, np. element nadrzędny może przenieść urządzenie końcowe do strefy odizolowanej (kwarantanny) w przypadku wykrycia anomalii.
           7. Integrację z podstawowym systemem kontroli dostępu znajdującym się na elemencie nadrzędnym. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: adresu mac, nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego, systemu operacyjnego, grupy użytkowników (w tym również możliwość integracji z zewnętrznym system LDAP – mapowanie grup).
           8. Przesyłanie logów na zewnętrzny serwer syslog.
     7. Moduły optyczne

Wraz z przełącznikami należy dostarczyć następujące moduły sieciowe światłowodowe. Ilość oraz typ została podana w tabeli zbiorczej. Moduły muszą być oficjalnie wspierane przez producenta urządzeń.

* 1. **Lista potrzebnych połączeń światłowodowych – interfejsy**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Urządzenie A | Urządzenie B | Prędkość | Medium | Rodzaj gniazda | Ilość interfejsów |
| „przełącznik główny” | „przełącznik dostępowy” | 10G | FO Single Mode | SFP+ | 160 szt. |
| „przełącznik główny” | „Kontroler urządzeń dostępowych i system bezpieczeństwa” | 100G | FO Single Mode | QSFP28 | 8 szt. |
| „przełącznik główny” | „przełącznik główny” | 100G | FO Single Mode | QSFP28 | 2 szt. |
| „Kontroler urządzeń dostępowych i system bezpieczeństwa” | „Kontroler urządzeń dostępowych i system bezpieczeństwa” | 10G | FO Single Mode | SFP+ | 6 szt. |
| „Kontroler urządzeń dostępowych i system bezpieczeństwa” | „przełącznik brzegowy” | 10G | FO Single Mode | SFP+ | 32 szt. |
| „przełącznik brzegowy” | „przełącznik brzegowy” | 100G BiDi | FO Single Mode | QSFP28 | 4 szt. |

# **Dostawa oprogramowania do urządzeń sieciowych - wymagania ogólne.**

# **Centralny system zarządzania:**

# W ramach postępowania wymagane jest dostarczenie centralnego systemu zarządzania przystosowanego do współpracy z systemami bezpieczeństwa sieciowego NGFW (Next Generation Firewall), posiadanymi przez Zamawiającego jak i oferowanym kontrolerem urządzeń dostępowych i systemem bezpieczeństwa. Centralny system zarządzania musi też w pełni zarządzać oferowanymi systemami opisywanymi w ramach tego postępowania, zarówno posiadanymi NGFW, urządzeniami typu kontroler urządzeń dostępowych i systemem bezpieczeństwa, jak i przełącznikami oraz posiadanymi Access Point.

# Centralny system zarządzania musi integrować się w sposób przygotowany przez producenta i wspierany z systemem kolekcji i korelacji logów.

# Rozwiązanie musi być dostarczone w postaci komercyjnej, kompletnej platformy programowej.

# Parametry wydajnościowe.

System musi umożliwiać zarządzenie:

* + - 1. NGFW posiadanymi przez zamawiającego w ilości 2 sztuki z 10 systemami wirtualnymi uruchomionymi na każdym z nich.
      2. oferowanym systemem kontroli urządzeń dostępowych i systemem bezpieczeństwa
      3. punktami dostępowymi WiFi.
      4. urządzeniami i systemami oferowanymi w ramach tego postępowania włączając w tą liczbę zarówno sprzętowe platformy, wirtualne systemy, jak i wirtualne instancje.

# Funkcjonalności centralnego systemu zarządzania.

W ramach centralnego systemu zarządzania muszą być realizowane co najmniej poniższe funkcje:

* + - 1. System centralnego zarządzania musi posiadać mechanizm zarządzania zmianami konfiguracji bazujący na osobnych rolach administratorów wykonujących konfigurację oraz rolach administratorów zatwierdzających zmiany, a także mechanizm audytu oraz porównywania konfiguracji i powiadamiania za pośrednictwem poczty elektronicznej o konfiguracji oczekującej na zatwierdzenie.
      2. System centralnego zarządzania musi dawać możliwość pełnej konfiguracji zarządzanych systemów NGFW i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa ze wszystkimi ich funkcjami składowymi.
      3. System centralnego zarządzania musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram instalowania zmian).
      4. System centralnego zarządzania musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
      5. System centralnego zarządzania musi umożliwiać sprawdzenie spójności polityki firewall (w tym m.in. wykrywanie zduplikowanych obiektów).
      6. System musi umożliwiać tworzenie dynamicznych obiektów (np. adresów IP), których wartość może być definiowana niezależnie per każdy zarządzany system bezpieczeństwa NGFW i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa.
      7. System centralnego zarządzania musi umożliwiać wyszukiwanie obiektów po ich nazwach oraz filtrowanie widoku polityki firewall na podstawie wybranych atrybutów reguł firewall.
      8. System centralnego zarządzania musi umożliwiać przypisywanie tych samych polityk firewall, profili bezpieczeństwa, polityk SD-WAN oraz wybranych ustawień systemowych do wielu zarządzanych systemów bezpieczeństwa NGFW i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa.
      9. System centralnego zarządzania musi umożliwiać tworzenie wielu wspólnych bloków polityk firewall, tzn. zestawów reguł firewall, które mogą być wykorzystane w wielu odrębnych politykach firewall przypisanych do różnych systemów bezpieczeństwa NGFW i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa. Administrator musi mieć możliwość umieszczenia takiego bloku w wybranym przez siebie miejscu polityki firewall.
      10. System centralnego zarządzania musi wersjonować konfiguracje w taki sposób, aby możliwe było odtworzenie wybranej konfiguracji zainstalowanej w przeszłości na systemie bezpieczeństwa NGFW i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa a obecnie przechowywanej w systemie centralnego zarządzania jako historyczna.
      11. System centralnego zarządzania musi umożliwiać zarządzanie wersjami firmware’u oraz zapewniać centralną aktualizację oprogramowania zarządzanych systemów NGFW jak i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa. Administrator musi mieć możliwość określenia daty automatycznej aktualizacji oprogramowania dla wybranych zarządzanych wyżej wymienionych systemów.
      12. System centralnego zarządzania musi oferować możliwość aktualizacji baz sygnatur na zarządzanych systemach NGFW i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa (wymienione zarządzane systemy nie muszą mieć dostępu do sieci Internet w celu aktualizacji swoich baz sygnatur).
      13. System centralnego zarządzania musi umożliwiać podgląd licencji (wraz z terminem ich ważności) na zarządzanych systemach bezpieczeństwa NGFW i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa.
      14. System centralnego zarządzania musi umożliwiać zdalne wykonywanie skryptów na zarządzanych systemach bezpieczeństwa. W skryptach powinna być możliwość wykorzystania zmiennych, których wartości przypisywane są niezależnie dla każdego zarządzanego systemu bezpieczeństwa NGFW jak i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa.
      15. System centralnego zarządzania musi umożliwiać monitoring zarządzanych systemów NGFW jak i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa. w zakresie m.in. aktualnych tablic routingu, funkcjonalności DHCP server, SD-WAN (opóźnienie, jitter, straty pakietów), statusu tuneli VPN IPSec.
      16. System centralnego zarządzania musi zawierać informacje, kiedy po raz pierwszy i kiedy po raz ostatni ruch przetwarzany przez zarządzane systemy NGFW i urządzenia typu kontroler urządzeń dostępowych i system bezpieczeństwa trafił w poszczególne reguły polityki firewall.
      17. System centralnego zarządzania musi umożliwiać zarządzanie systemami NGFW i urządzeniami typu kontroler urządzeń dostępowych i system bezpieczeństwa znajdującymi się za NAT.
      18. System centralnego zarządzania musi umożliwiać uruchamianie systemów NGFW w trybie ZTP (Zero Touch Provisioning).
      19. System musi optymalizować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mesh poprzez obiekty typu community/topologie VPN, umożliwiające proste dodawanie zarządzanych urządzeń w celu dołączenia ich do danej topologii VPN.
      20. System zarządzania musi mieć możliwość pracy w trybie klastra niezawodnościowego, złożonego przynajmniej z dwóch elementów. Konfiguracja zarządzanych urządzeń musi być automatycznie synchronizowana pomiędzy wszystkimi elementami tego klastra.
      21. System centralnego zarządzania musi mieć możliwość podziału na wirtualne systemy zarządzania (konteksty), które będą posiadały odrębne definicje obiektów. Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych wirtualnych systemów zarządzania.
      22. System centralnego zarządzania musi umożliwiać pracę wielu administratorów jednocześnie. System musi mieć możliwość blokady kontekstu (domeny administracyjnej), aby różni administratorzy nie mogli wykonywać w tym samym czasie zmian w tym samym kontekście. Administrator musi mieć także możliwość blokady tylko wybranej polityki firewall w obrębie całego kontekstu.
      23. W przypadku pracy w trybie z kontekstami (domenami administracyjnymi) musi istnieć możliwość definiowania globalnych obiektów (np. adresów IP, portów TCP/UDP, profili bezpieczeństwa), które będą dostępne w wybranych kontekstach i gotowe do użycia np. w politykach firewall.
      24. System musi pozwalać na włączanie lub wyłączanie widoczności w GUI systemu centralnego zarządzania wybranych elementów konfiguracji zarządzanych urządzeń.
      25. System musi pozwalać na łatwą zamianę zarządzanego urządzenia NGFW jak i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa, które uległo awarii, na nowe urządzenie tego samego modelu bez konieczności ponownego wykonywania jego pełnej konfiguracji czy ręcznego przenoszenia konfiguracji.

# Zarządzanie.

# System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.

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

# System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do wybranych elementów zarządzania oraz wybrania zarządzanych systemów dostępnych dla tego administratora.

# Komunikacja pomiędzy systemem centralnego zarządzania a zarządzanymi systemami NGFW oraz i urządzeniami typu kontroler urządzeń dostępowych i system bezpieczeństwa musi odbywać się w sposób szyfrowany.

# System musi posiadać API, które umożliwia zarówno zarządzenie urządzeniami podłączonymi do systemu jak i samym systemem centralnego zarządzania.

# **C****entralny system do kolekcji i korelacji logów - wymagania ogólne.**

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

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy programowej.

# Parametry wydajnościowe.

# System musi być w stanie przyjmować minimum 25 GB logów na dzień.

# Rozwiązanie musi umożliwiać kolekcjonowanie logów z wszystkich oferowanych systemów oraz posiadanych przez Zamawiającego NGFW jak i oferowanych urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa.

# Funkcjonalności Systemu:

# Podgląd logowanych zdarzeń w czasie rzeczywistym.

# Możliwość przeglądania logów historycznych z funkcją filtrowania.

# Możliwość dostosowania widoku wyświetlanych logów poprzez dodawanie, usuwanie oraz zmianę kolejności kolumn zawierających elementy logowanego zdarzenia.

# System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia NGFW i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa na przestrzeni zadanego czasu. Muszą one obejmować co najmniej:

# Listę najczęściej wykrywanych ataków.

# Listę najbardziej aktywnych użytkowników/źródeł ruchu.

# Listę najczęściej wykorzystywanych aplikacji.

# Listę najczęściej odwiedzanych stron www.

# Listę krajów, do których nawiązywane są połączenia.

# Listę najczęściej wykorzystywanych polityk Firewall.

# Informacje o realizowanych połączeniach IPSec i SSL VPN.

# Listę najczęściej występujących zdarzeń systemowych.

# Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych za pomocą protokołu Syslog i/lub CEF. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.

# Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem portów UDP/514 oraz TCP/514.

# System musi umożliwiać cykliczny eksport logów do zewnętrznego systemu w celu ich długoterminowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP i/lub SCP. Administrator musi mieć możliwość określenia, kiedy ma następować eksport logów.

# System musi prezentować informacje na temat ilości przestrzeni dyskowej wykorzystanej na przechowywanie logów.

# Raportowanie.

W zakresie raportowania system musi zapewniać:

# Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.

# Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.

# Funkcję definiowania własnych raportów.

# Możliwość spolszczenia raportów.

# Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email oraz automatycznego przesłania raportu na zewnętrzny serwer za pomocą protokołu FTP lub SCP.

# Możliwość filtrowania danych uwzględnianych w procesie tworzenia danego raportu, m.in. możliwość ograniczenia zakresu raportu do danych z wybranych urządzeń NGFW jak i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa a także z wybranej adresacji IP.

# Możliwość automatycznego usuwania raportów po określonym czasie.

# Korelacja logów.

W zakresie korelacji zdarzeń system musi zapewniać:

# Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.

# Możliwość tworzenia własnych reguł korelowania logów.

# Konfigurację powiadomień poprzez: e-mail, SNMP oraz API http w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. W treści powiadomienia musi być możliwość przekazania dodatkowych informacji o zdarzeniu wywołującym dane powiadomienie, np. nazwa wykrytego zagrożenia.

# Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

# Malware/AV.

# Aplikacje sieciowe.

# Email.

# IPS.

# Web Filter.

# Traffic (logi z ruchu sieciowego).

# Systemowe (m.in. utracone połączenie VPN, utracone połączenie sieciowe, zdarzenia związane z klastrem niezawodnościowym, zmiana w sieci SD-WAN).

# Możliwość automatycznego, zwrotnego powiadomienia systemu bezpieczeństwa NGFW jak i urządzeń typu kontroler urządzeń dostępowych i system bezpieczeństwa o wystąpieniu wybranych zdarzeń korelacji.

# System musi automatycznie aktualizować informacje o IoC (tzw. wskaźniki kompromitacji) dostarczanymi przez producenta rozwiązania w regularnych aktualizacjach. Informacje te wykorzystywane są do korelacji zgromadzonych przez system zdarzeń w celu wykrycia podejrzanych zachowań. IoC powinny zawierać informacje o złośliwych adresach IP, domenach oraz adresach URL. Licencja powinna upoważniać do korzystania z subskrypcji przez okres 36 miesięcy.

# Funkcje pracy w trybie wysokiej dostępności (HA).

Wymaganym jest aby system centralnego logowania miał możliwość pracy w trybie klastra z następującymi funkcjami

# Tryb synchronizacji zdarzeń (logów) pomiędzy urządzeniami klastra HA.

# Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.

# Monitorowanie stanu pracy klastra HA.

# Umożliwiać wykorzystanie urządzenia pasywnego klastra HA do wykonywania niektórych zadań, pozwalających na redukcję obciążenia urządzenia głównego (w szczególności w zadaniu generowania raportów).

# Zarządzanie.

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

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

# System musi umożliwiać definiowanie co najmniej 5 administratorów z możliwością określenia praw dostępu do wybranych modułów systemu logowania i raportowania.

# System musi mieć możliwość podziału na wirtualne systemy logowania i raportowania (konteksty/domeny). Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych kontekstów. Dla każdego kontekstu musi być możliwość niezależnego przydzielania zasobów dyskowych oraz określania maksymalnego czasu przechowywania logów

# **Wdrożenie urządzeń i oprogramowania, w tym instalacja i konfiguracja.**

# Wykonawca zobowiązuje się do wdrożenia urządzeń zgodnie z poniższym opisem.

# Analiza i projekt wdrożenia:

# Analiza obecnej konfiguracji sieci, wykorzystywanego rozwiązania firewall wraz z przeglądem istniejącej dokumentacji administratorskiej.

# Analiza i uwzględnienie aktualnych ustawień posiadanych Firewall sprzętowych oraz innych aktywnych urządzeń sieciowych (np. WiFi).

# Analiza integracji systemu z zasobami Zamawiającego, w tym:

# dystrybucja i konfiguracja klientów VPN użytkowników,

# integracja z AD, Forti Analyzer, użytkownymi przez Zamawiającego,

# konfiguracja kanałów VPN site to site,

# integracja i zarządzanie urządzeniami Access Point WiFi,

# analiza systemów DMZ,

# integracja z zasobami chmury Azure Zamawiającego.

# Analiza potrzeb i wymagań systemu bezpieczeństwa infrastruktury dostępowej będących przedmiotem zamówienia.

# Propozycje i zalecenia do bieżącego wdrożenia, możliwe do zastosowania w przyszłości.

# Wykonanie projektu technicznego wdrożenia. Przed konfiguracją dostarczonych urządzeń.

# Zamawiający w terminie 5 dni roboczych od otrzymania projektu technicznego dokona jego akceptacji lub zgłosi uwagi. Warunkiem rozpoczęcia prac wdrożeniowych jest zaakceptowanie przez Zamawiającego projektu technicznego.

# Przeprowadzanie warsztatów omawiających zakres wdrożenia oraz proponowaną konfigurację sieci i urządzeń Systemu.

# Instalacja i prace wdrożeniowe.

# Dostawa i rozładunek urządzeń w siedzibie Zamawiającego.

# Montaż i podstawowa konfiguracja dostarczanych urządzeń w infrastrukturze Zamawiającego.

# Przeniesienie/odwzorowanie istniejących usług z obecnego rozwiązania Firewall na dostarczane urządzenia. Odwzorowanie powinno zawierać ustalenia z zaakceptowanego projektu technicznego wdrożenia.

# Integracja z systemami wewnętrznymi Zamawiającego, w tym z AD, Forti Analyzer, oraz innymi zasobami wymienionymi w procesie analizy.

# Przeniesienie funkcjonalności kontrolera Access Pointów na dostarczone urządzenia.

# Konfiguracja stref bezpieczeństwa.

# Migracja lub stworzenie usług w wewnętrznej sieci LAN.

# Konfiguracja routingu oraz styku z siecią Internet.

# Migracja lub stworzenie reguł firewall, w tym: IPS, aplikacyjnych, i ich optymalizacja.

# Migracja lub stworzenie usług VPN site-to-site (dla 2 lokalizacji).

# Migracja lub stworzenie usługi VPN na urządzenia pracowników zamawiającego i przygotowane szablonu konfiguracji dla aplikacji klienta VPN.

# Niezbędne prace rekonfiguracyjne w sieci informatycznej Zamawiającego.

# Przełączanie usług na dostarczane urządzenia Systemu bezpieczeństwa.

# Stopniowe przełączanie usług i sieci – w uzgodnionym przez Strony terminie.

# Testy uruchomieniowe po przełączeniu usług, następnie testy akceptacyjne.

# Przeprowadzenie zewnętrznych testów podatności sieci.

# Optymalizacja konfiguracji.

# Uaktualnienia firmware'u dostarczonych urządzeń do najnowszej wersji.

# Wykonanie i przekazanie Zamawiającemu dokumentacji.

# Przeprowadzenie końcowych testów odbiorczych.

# Przeszkolenie maksymalnie do 10 administratorów Zamawiającego z eksploatacji, konfiguracji Systemu, w formie dwóch spotkań po minimum 1 dzień, w uzgodnionym przez Strony terminie.

# Konfiguracja urządzeń typu „przełącznik brzegowy” w celu połącznia nowej infrastruktury z istniejącą infrastrukturą sieciową dedykowanymi światłowodami lub poprzez sieć Internet kanałami VPN site to site.

# Konfiguracja innych urządzeń oraz elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej będących przedmiotem zamówienia zgodnie z projektem wdrożenia.

# Zapewnienie konsultacji dot. oferowanego rozwiązania (z czego minimum 1/3 oferowanych dni/godzin realizowana jest i na miejscu u Zamawiającego) przez cały okres obowiązywania umowy.

# Wykonawca posiada i oddeleguje do realizacji prac realizacji min. 2 inżynierów z certyfikatem z najwyższym lub minimum „najwyższym -1” w zakresie rozwiązań bezpieczeństwa sieciowego. Np.: CCIE, NSE 7, JNCIS-SEC, itp.

# Wykonawca jest doświadczonym i profesjonalnym dostawcą oferowanych rozwiązań danego producenta (które oferuje w niniejszym postępowaniu) i legitymuje się aktualnym statusem partnerskim producenta na poziomie najwyższym lub minimum „najwyższym -1”.

# **Zapewnienie 3-letniego pakietu gwarancyjnego i licencyjnego.**

* 1. Urządzenia objęte będą min. 3-letnią gwarancją producenta oraz 3-letnią licencją na funkcjonalności opisane w niniejszej dokumentacji, w tym aktualizację oprogramowania urządzeń.
  2. Przez cały okres gwarancji Zamawiający ma dostęp do najnowszych wersji oprogramowania urządzeń
  3. Wsparcie serwisowe musi być objęte serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości z czasem na dostawę nowego urządzenia w terminie 4h od potwierdzenia przyjęcia zgłoszenia w systemie suportowym producenta. W ramach serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
  4. Obsługa zdarzeń rejestrowanych w systemie suportowym producenta gdzie czas odpowiedzi producenta na zgłoszenie jest adekwatny do ważności usterki i spełnia poniższe kryteria:
     1. do 15 minut w przypadku zgłoszeń o priorytecie najwyższy/wysoki,
     2. poniżej 2 godzin roboczych w przypadku zgłoszeń o priorytecie średni.
  5. Dla priorytetu niski poniżej 4 godzin roboczych.
  6. W przypadku braku możliwości rozwiązania problemu „ad-hoc”, serwis producenta zaproponuje rozwiązanie tymczasowe usterki do czasu usunięcia awarii/usterki.
  7. W przypadku wadliwości urządzenia lub niestabilności jego działania pakiet gwarancyjny zapewnia naprawę (w tym również wymianę) urządzenia w terminie do końca następnego dnia roboczego od zgłoszenia.
  8. Na czas naprawy Zamawiający akceptuje urządzenie zastępcze o nie gorszej funkcjonalności, po jego odpowiedniemu skonfigurowaniu (odpowiadającemu konfiguracji urządzenia zastępowanego) przez Wykonawcę lub inny podmiot upoważniony przez producenta Systemu (lub jego przedstawiciela).
  9. Przez cały okres gwarancji Zamawiający ma dostęp do najnowszych wersji oprogramowania urządzeń.
  10. Naprawy mogą być realizowane przez producenta, Wykonawcę lub inny podmiot upoważniony przez producenta. Naprawa urządzeń odbywać się będzie w miejscu wskazanym przez Zamawiającego. Naprawa może odbyć się w serwisie, jeżeli Wykonawca uzna to za konieczne, przy czym Wykonawca transportuje uszkodzony sprzęt do serwisu, a po naprawie z serwisu, na własny koszt i ryzyko.
  11. Po wykonaniu napraw urządzeń poza siedzibą Zamawiającego, Wykonawca zobowiązuje się dokonać ponownej instalacji sprzętu w środowisku Zamawiającego.
  12. Zgłoszenia serwisowe mogą być dokonywane w języku polskim, 24 godziny na dobę, przez wszystkie dni w tygodniu.
  13. Pakiet gwarancyjny zapewnia naprawę lub wymianę urządzeń, lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta.

# O ile Strony nie uzgodnią inaczej, wszelkie usługi gwarancyjne, w tym naprawy i wymiany gwarancyjne, będą realizowane w siedzibie Zamawiającego w dni robocze, w godzinach 7.30-15.30.

# **Usługi wsparcia Wykonawcy**

# Przez okres obowiązywania umowy (albo do wyczerpania puli godzin wsparcia, w zależności co nastąpi wcześniej) Wykonawca będzie realizował usługi wsparcia do Systemu.

* 1. Pula godzin wsparcia wynosi 600, przy czym Zamawiający zobowiązuje się do wykorzystania co najmniej 300 godzin.
  2. O ile Strony nie uzgodnią inaczej, wsparcie będzie realizowane w dni robocze w godzinach 7.30 - 15.30.
  3. W sytuacjach wyjątkowych, wsparcie może być realizowane o innej porze niż określono powyżej. W takim przypadku Zamawiający poinformuje Wykonawcę 5 dni roboczych wcześniej. Szczegóły Strony będą uzgadniały na roboczo.
  4. Wsparcie może być realizowane zdalnie lub w siedzibie Zamawiającego – jeżeli realizacja zdalnie nie będzie możliwa lub będzie nieefektywna.
  5. O ile Strony nie uzgodnią w danym przypadku inaczej, wsparcie będzie realizowane zgodnie z procedurą:
     1. Zamawiający prześle Wykonawcy potrzebę wsparcia, z opisem potrzeby.

# Wykonawca w terminie 2 dni roboczych odpowie na przesłaną potrzebę i ustali z Zamawiającym szczegóły tej potrzeby.

# W terminie 2 dni roboczych od ustalenia szczegółów potrzeby, specjaliści Wykonawcy przystąpią do realizacji wsparcia.

# W sytuacji nieprzewidzianej i potrzebie natychmiastowej realizacji wsparcia, pierwsze dwie godziny takiego wsparcia liczone będą podwójnie (godzina takiego wsparcia będzie odpowiadała dwóm godzinom świadczenia usługi wsparcia określonej w umowie z Wykonawcą).

# Wsparcie obejmować będzie między innymi:

# Koordynowanie zgłoszenia gwarancyjnego poprzez przygotowanie i przekazanie zgłoszenia producentowi/serwisowi, monitorowanie zgłoszenia.

# Prace rekonfiguracyjne, diagnostycznie i projektowe.

# Opracowanie przez Wykonawcę dokumentacji dotyczącej zrealizowanego świadczenia.

# Przeprowadzenia aktualizacji oprogramowania Urządzeń.

# Warsztaty/przeszkolenia w dziedzinach związanych z działaniem Urządzeń oraz całej infrastruktury Firewall, WiFi, VPN oraz elementów powiązanych z tą infrastrukturą.

# Strony uzgodnią każdorazowo przed realizacją zlecenia, wstępny szacunek pracochłonności - liczbę godzin przewidywaną na realizację zlecenia. Dopuszcza się różnicę w liczbie godzin przedstawionej w protokole realizacji zlecenia, a wstępnym szacunkiem pracochłonności, w zakresie +/- 20 %.