OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiot zamówienia: Dostawa urządzeń i oprogramowania bezpieczeństwa wraz z niezbędnymi licencjami oraz usługą konfiguracji i integracji sprzętu z infrastrukturą ITWL – 1 komplet.

Specyfikacja przedmiotu zamówienia – charakterystyka, parametry techniczne, cechy funkcjonalne przedmiotu zamówienia – parametry minimalne:

Zakres: *Dostawa do siedziby Zamawiającego fabrycznie nowych, nieużywanych, pochodzących z bieżącej produkcji, urządzeń sieciowych wraz z konfiguracją, szkoleniem administratorów oraz niezbędnymi licencjami w ramach etapu 2 projektu modernizacji infrastruktury IT dla ITWL***.**

I. Zarządzalny Firewall NGFW (model przykładowy: FortiGate 100F) - 2 szt.

1. **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, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
   System musi wspierać IPv4 oraz IPv6 w zakresie:
   1) Firewall.
   2) Ochrony w warstwie aplikacji.
   3) Protokołów routingu dynamicznego.
2. **Redundancja, monitoring i wykrywanie awarii:**
   1) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
   2) W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
   3) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

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

3. Interfejsy, Dysk, Zasilanie:

1) System realizujący funkcję Firewall musi dysponować minimum:
   a) 16 portami Gigabit Ethernet RJ-45.
   b) 8 gniazdami SFP 1 Gbps.
   c) 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.

4. Parametry wydajnościowe:

1) W zakresie Firewall obsługa nie mniej niż 1.5 min. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2) Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4) Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
5) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno Client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - minimum 1 Gbps.

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) Kontrola Aplikacji.
3) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4) Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5) Ochrona przed atakami - Intrusion Prevention System.
6) Kontrola stron WWW.
7) Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3.
8) Zarządzanie pasmem (QoS, Traffic shaping).
9) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10) Dwuskładnikowe 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.
11) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12) Analiza ruchu szyfrowanego protokołem SSH.
13) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

6. Polityki, Firewall:

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:
   a) Translację jeden do jeden oraz jeden do wielu.
   b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5) Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   a) Amazon Web Services (AWS).
   b) Microsoft Azure
   c) Google Cloud Platform (GCP).
   d) OpenStack.
   e) VMware NSX.
   f) Nutanix.

7. Połączenia VPN:

1) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   a) Wsparcie dla IKE v1 oraz v2.
   b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM).
   c) Obsługa protokołu Diffie-Hellman grup 19 i 20.
   d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
i) Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
a) 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.
b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

8. Routing i obsługa łączy WAN:

1) W zakresie routingu rozwiązanie powinno zapewniać obsługę:
a) Routingu statycznego.
b) Policy Based Routingu.
c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

9. Funkcje SD-WAN:

1) System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2) Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

10. Zarządzanie pasmem:

1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

11. Ochrona przed malware:

1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona

platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

5) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

12. Ochrona przed atakami:

1) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3) Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

13. Kontrola aplikacji:

1) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2) Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4) Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

14. 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, Dynamie DNS, proxy.
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) Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7) W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

15. Uwierzytelnianie użytkowników w ramach sesji:

1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

16. 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 dwuskładnikowego dla dostępu administracyjnego.
4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6) Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7) Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie

zostaną zatwierdzone.

17. Logowanie

1) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4) Musi istnieć możliwość logowania do serwera SYSLOG.

18. Certyfikaty:

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

a) ICSA lub EAL4 dla funkcji Firewall.

19. Serwisy i licencje:

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

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

20. Gwarancja oraz wsparcie:

1) Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

21. Rozszerzone wsparcie serwisowe AHB/SOS:

1) System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.
2) Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:

a) 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).
b) Certyfikat ISO 9001 podmiotu serwisującego.

II. Zarządzalny przełącznik L2 (model przykładowy: FortiSwitch 124F) - 1 szt.

1. Przełącznik sieciowy:

W ramach postępowania wymaganym 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 przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:

2. Parametry fizyczne platformy:

1) Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
2) Zasilanie AC 230V.
3) Maksymalny pobór mocy: 30 W.
4) Minimalny zakres temperatury pracy: 0-40°C.

3. Interfejsy sieciowe - wymagania minimalne:

1) Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
a) 24 porty GE RJ-45.
b) 4 porty 10GESFP+.

4. Zarządzanie:

1) Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
2) Zarządzanie przez: command linę (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
3) Wsparcie dla SNMP w wersjach 1-3
4) Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
5) Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
6) Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
7) Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
8) Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
9) Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko

odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.

10) Automatycznie wykonywane rewizje konfiguracji.

5. Parametry wydajnościowe:

1) Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mbps.
2) Tablica adresów MAC o pojemności co najmniej 32k wpisów.
3) Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

6. Wymagane funkcje:

1) Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
2) Obsługa Jumbo Frames.
3) Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
4) Agregacja portów zgodna ze standardem 802.3ad.
5) Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.10.
6) Port-mirroring.
7) Uwierzytelnianie 802.1 x na poziomie portu.
8) Uwierzytelnianie 802.1x w oparciu o adres MAC.
9) W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
10) W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
11) W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
12) Obsługa protokołu sFlow.

7. Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:

1) Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   a) Centralne zarządzanie konfiguracją urządzenia
   b) Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   c) Centralne zarządzanie sieciami VLAN.
   d) Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   e) Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
   f) Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   g) Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie

na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.

h) Automatyczna detekcja i rekomendacje konfiguracji.
i) Przesyłanie logów na zewnętrzny serwer syslog.
j) Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
k) Obsługa białych i czarnych list adresów MAC.
l) Wykrywanie aplikacji komunikujących się w sieci.

2) Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3) W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

8. Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:

1) System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
2) System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

9. Gwarancja oraz wsparcie:

1) System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

10. Rozszerzone wsparcie serwisowe:

1) System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.
2) Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:
   a) 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).
   b) Certyfikat ISO 9001 podmiotu serwisującego.

III. Zarządzalny Firewall NGFW (model przykładowy: FortiGate 60F LUB 80F) - 1 szt.

1. **Wymagania ogólne:**
    1) 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.
    2) System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
    3) W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
    4) System musi wspierać IPv4 oraz IPv6 w zakresie:
        a) Firewall.
        b) Ochrony w warstwie aplikacji.
        c) Protokołów routingu dynamicznego.
2. **Redundancja, monitoring i wykrywanie awarii:**
    1) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
    2) W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
    3) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
    4) Monitoring stanu realizowanych połączeń VPN.
    5) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
3. **Interfejsy, Dysk, Zasilanie:**
    1) System realizujący funkcję Firewall musi dysponować minimum:
        a) m.in. 8 portami Gigabit Ethernet RJ-45.
        b) opcjonalnie min 2 portami SFP 1 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.
4. **Parametry wydajnościowe:**

1) W zakresie Firewall obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz min. 35 tys. nowych połączeń na sekundę.
2) Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4) Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
5) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http - minimum 600 Mbps.

5. Funkcje Systemu Bezpieczeństwa:

1) W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
b) Kontrola Aplikacji.
c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
d) Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
e) Ochrona przed atakami - Intrusion Prevention System.
f) Kontrola stron WWW.
g) Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3.
h) Zarządzanie pasmem (QoS, Traffic shaping).
i) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
j) Dwuskładnikowe 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.
k) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
l) Analiza ruchu szyfrowanego protokołem SSH.
m) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

6. Polityki, Firewall:

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:

a) Translację jeden do jeden oraz jeden do wielu.
b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5) Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   a) Amazon Web Services (AWS).
   b) Microsoft Azure
   c) Google Cloud Platform (GCP).
   d) OpenStack.
   e) VMware NSX.
   f) Nutanix.

7. Połączenia VPN:

1) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   a) Wsparcie dla IKE v1 oraz v2.
   b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM).
   c) Obsługa protokołu Diffie-Hellman grup 19 i 20.
   d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tunel.
   e) pomiędzy SPOKE w topologii HUB and SPOKE.
   f) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   g) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   h) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   i) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   j) Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   a) 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.
   b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy

zastosowaniu dedykowanego klienta.

c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

8. Routing i obsługa łączy WAN:

1) W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   a) Routingu statycznego.
   b) Policy Based Routingu.
   c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

9. Funkcje SD-WAN:

1) System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2) Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

10. Zarządzanie pasmem:

1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

11. Ochrona przed malware:

1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

12. Ochrona przed atakami:

1) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3) Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana

automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

13. Kontrola aplikacji:

1) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2) Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4) Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

14. 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, Dynamie DNS, proxy.
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) Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

15. Uwierzytelnianie użytkowników w ramach sesji:

1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z

LDAP.

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

2) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http.

16. 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 dwuskładnikowego dla dostępu administracyjnego.
4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6) Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7) Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

17. Logowanie:

1) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4) Musi istnieć możliwość logowania do serwera SYSLOG.

18. Certyfikaty:

1) Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:
   a) ICSA lub EAL4 dla funkcji Firewall.

19. Serwisy i licencje:

1) W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
   a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

20. Gwarancja oraz wsparcie:

System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

21. Rozszerzone wsparcie serwisowe AHB/SOS:

1) System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres [x] miesięcy.
2) Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:
   a) 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).
   b) Certyfikat ISO 9001 podmiotu serwisującego.

IV. Zarządzalne światłowodowe przełączniki L3 (model przykładowy: FortiSwitch FS-1048E) - 3 szt.

1. Przełącznik sieciowy:

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Zamawiający jest w posiadaniu rozwiązania FortiGate. W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z istniejącym rozwiązaniem FortiGate, o następujących parametrach:

2. Parametry fizyczne platformy:

1) Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
2) Zasilanie AC 230V.
3) Wymagany - z możliwością wymiany w czasie pracy - redundantny zasilacz.
4) Maksymalny pobór mocy: 185 W.
5) Minimalny zakres temperatury pracy: 0-40°C.

3. Interfejsy sieciowe - wymagania minimalne:

1. Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty 10 GE SFP+
b) 6 porty 40 GE QSFP+
c) 4 porty 100 GE QSFP28

4. Zarządzanie:

1) Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
2) Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
3) Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
4) Wsparcie dla SNMP w wersjach 1-3
5) Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania,
6) pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
7) Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
8) Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
9) Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
10) Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
11) Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
12) Automatycznie wykonywane rewizje konfiguracji.

5. Parametry wydajnościowe:

1) Przepustowość urządzenia - min. 1750 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 1515 Mbps.

2) Tablica adresów MAC o pojemności co najmniej 144 k wpisów.
3) Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

6. Wymagane funkcje:

1) Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
2) Obsługa Jumbo Frames.
3) Obsługa 802.Id (Spanning Tree), 802.Iw (Rapid Spanning Tree), 802.Is (Multiple Spanning Tree).
4) Agregacja portów zgodna ze standardem 802.3ad.
5) Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
6) Obsługa routingu statycznego.
7) Obsługa Ouality of Service, w tym zakresie: 802.lp oraz DSCP.
8) Port-mirroring.
9) Uwierzytelnianie 802.lx na poziomie portu.
10) Uwierzytelnianie 802.lx w oparciu o adres MAC.
11) W ramach 802.lx wsparcie dla dedykowanego VLANu dla gości (guest VLAN).
12) W ramach 802.lx wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
13) W ramach 802.lx wsparcie dla dynamicznego przypisywania VLAN.
14) Obsługa protokołu sFlow.

7. Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:

1) Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   a) Centralne zarządzanie konfiguracją urządzenia.
   b) Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania.
   c) Centralne zarządzanie sieciami VLAN.
   d) Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u.
   e) Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
   f) Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   g) Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
   h) Automatyczna detekcja i rekomendacje konfiguracji.
   i) Przesyłanie logów na zewnętrzny serwer syslog.

j) Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.

k) Obsługa białych i czarnych list adresów MAC.

l) Wykrywanie aplikacji komunikujących się w sieci.

2) Musi być możliwe redundantne połączenie z elementami zarządzającymi.

3) W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

8. Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:

1) System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.

2) System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

9. Gwarancja oraz wsparcie:

System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

10. Rozszerzone wsparcie serwisowe:

1) System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.

2) Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:

a) 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).

b) Certyfikat ISO 9001 podmiotu serwisującego.

V. Zarządzalny wirtualny Firewall NGFW (model przykładowy: FortiGate VM02V KVM) — 3 szt.

1. Wymagania Ogólne:

1) 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 wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy wirtualne wraz z odpowiednio zabezpieczonym systemem operacyjnym. Platformy wirtualne muszą wspierać następujące rodzaje hypervisorów: ESXi v5.5 lub wyższe, XenServer v6.0 lub wyższe, Hyper-V 2008R2 lub wyższe, AWS, Azure, CentOS v6.4 lub wyższe, KVM libvirt 0.10.2 lub wyższe, Nautanix.

2) System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT oraz transparentnym.
3) W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość rozbudowy do minimum 22 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. W ramach postępowania wymaganym jest dostarczenie licencji umożliwiających uruchomienie 3 instancji systemu.
4) Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
5) System musi wspierać IPv4 oraz IPv6 w zakresie:
   a) Firewall.
   b) Ochrony w warstwie aplikacji.
   c) Protokołów routingu dynamicznego.

2. 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) Monitoring i wykrywanie uszkodzenia elementów programowych systemów zabezpieczeń oraz łączy sieciowych.
3) Monitoring stanu realizowanych połączeń VPN.
4) System musi umożliwiać statyczną agregację linków.

3. Interfejsy, Dyski, Procesory, Pamięć:

1) System musi obsługiwać co najmniej 10 interfejsów sieciowych oraz wspierać powierzchnię dyskową o pojemności 2 TB.
2) System musi obsługiwać co najmniej 4 GB pamięci RAM oraz ilość procesorów: 2.
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. Parametry wydajnościowe:

1) W zakresie Firewall obsługa nie mniej niż 120 tyś. nowych połączeń na sekundę.
2) Przepustowość Stateful Firewall: nie mniej niż 17 Gbps.

3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3 Gbps.
4) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno Client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Mix - minimum 2.8 Gbps.
5) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control - minimum 2.1 Gbps.
6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps.
7) Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA1: nie mniej niż 2.2 Gbps.

5. Funkcje Systemu Bezpieczeństwa:

1) W ramach dostarczonego systemu ochrony musi istnieć możliwość uruchomienia poniższych funkcji. W przypadku, kiedy do ich uruchomienia niezbędne są licencje -muszą one zostać dostarczone stosownie do wymagań z sekcji "Serwisy i Licencje". Mogą one być zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub programowych.
2) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
3) Kontrola Aplikacji.
4) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
5) Ochrona przed malware - co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
6) Ochrona przed atakami - Intrusion Prevention System.
7) Kontrola stron WWW.
8) Kontrola zawartości poczty - Antyspam dla protokołów SMTP, POP3.
9) Zarządzanie pasmem (QoS, Traffic shaping).
10) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
11) Dwuskładnikowe 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.
12) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
13) Analiza ruchu szyfrowanego protokołem SSH.
14) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

6. Polityki, Firewall:

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:

a) Translację jeden do jeden oraz jeden do wielu.
b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5) Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   a) Amazon Web Services (AWS).
   b) Microsoft Azure
   c) Google Cloud Platform (GCP).
   d) OpenStack.
   e) VMware NSX.
   f) Nutanix.

7. Połączenia VPN:

1) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   a) Wsparcie dla IKE v1 oraz v2.
   b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM).
   c) Obsługa protokołu Diffie-Hellman grup 19 i 20.
   d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   i) Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   a) 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.
   b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

8. Routing i obsługa łączy WAN:

1) W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   a) Routingu statycznego.
   b) Policy Based Routingu.
   c) 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.
3) Reguły zarządzania rozkładem obciążenia powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

9. Zarządzanie pasmem:

1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

10. Ochrona przed malware:

1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

11. Ochrona przed atakami:

1) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3) Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

12. Kontrola aplikacji:

1) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2) Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4) Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

13. Kontrola WWW:

1) Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2) W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamie DNS, proxy.
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) Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7) W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

14. Uwierzytelnianie użytkowników w ramach sesji:

1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

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

2) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

15. Zarządzanie:

1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3) Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6) Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7) Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

16. Logowanie:

1) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4) Musi istnieć możliwość logowania do serwera SYSLOG.

17. Certyfikaty:

1) Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:
   a) ICSA lub EAL4 dla funkcji Firewall.

18. Serwisy i licencje:

1) System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania i dostępu do baz bezpieczeństwa.
2) W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

19. Gwarancja oraz wsparcie:

1) Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy. W ramach tego serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

20. Rozszerzone wsparcie serwisowe AHB/SOS:

1) System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.
2) Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:
   a) 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).
   b) Certyfikat ISO 9001 podmiotu serwisującego.

VI. Centralny system zarządzania, logowania i korelacji zdarzeń (model przykładowy: FortiAnalyzer FAZ-VM-GB5-SUBSC) - 3 szt.

1. Wymagania Ogólne:

1) 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.

2) 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 wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper- V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

2. Interfejsy, Dysk:

1) System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.

3. Parametry wydajnościowe:

1) System musi być w stanie przyjmować minimum 5 GB logów na dzień (15GB w zakresie wszystkich dostarczonych licencji).
2) Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

4. 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 długotrwałego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

5. Raportowanie:

W zakresie raportowania system musi zapewniać:

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

6. 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 powinien korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   a) Malware.
   b) Aplikacje sieciowe.
   c) Email.
   d) IPS.
   e) T raffic.
   f) Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

7. 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 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

8. Serwisy i licencje:

1) Wsparcie: System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

VII. Systemu centralnego zarządzania oraz logowania i raportowania (model przykładowy: FortiManager FMG-10-UG) - 1 szt.

1. Wymagania Ogólne:

1) W ramach postępowania wymaganym jest dostarczenie systemu centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z systemem bezpieczeństwa sieciowego (np. NGFW).
2) Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy lub komercyjnych platform działających w środowisku wirtualnym lub w postaci komercyjnej platformy/komercyjnych platform działających na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX, ESXi wersje: 5.5,6.0,6.5,6.7; Microsoft Hyper-V 2012, 2016; Citrix XenServer 6.0+; Open Source Xen 4.1+; KVM Redhat 6.5+, Amazon Web Services (AWS), Microsoft Azure, Google Cloud.

2. Interfejsy, Dysk:

1) System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 200 GB.

3. Parametry wydajnościowe:

1) System musi umożliwiać zarządzenie co najmniej 10 systemami bezpieczeństwa.
2) Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 10 systemów.
3) System musi być w stanie przyjmować minimum 2 GB logów na dzień.

4. Funkcje systemu centralnego Zarządzania:

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

1) System musi posiadać system zarządzenia zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji).
2) System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi.
3) System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian).
4) System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
5) System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.
6) System musi umożliwiać zarządzenie wersjami firmware'u oraz zapewniać centralną aktualizację oprogramowania.
7) System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń.
8) System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia).
9) System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami.
10) System musi zapisywać i zdalne wykonywać skrypty na urządzeniach.
11) System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM).

12) System musi automatyzować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mash.
13) Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

5. Funkcje logowania:

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.

6. Funkcja raportowania:

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) Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

7. Funkcje korelacji:

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 powinien korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   a) Malware.
   b) Aplikacje sieciowe.
   c) Email.
   d) IPS.
   e) T raffic.
   f) Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

8. **Zarządzanie:**
    1) System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
        a) Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI.
    2) System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów zarządzania z perspektywy poszczególnych zarządzanych systemów.
    3) System musi posiadać API które umożliwia zarządzenie urządzeniami podłączonymi do systemu za pomocą poleceń REST API.
    4) Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
9. **Gwarancja oraz wsparcie:**
    1) System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
    2) Wsparcie: System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

VIII. 10GBASE-LR SFP+ 850nm 10km DOM LC MMF Transceiver Module Wkładki światłowodowe do FortiGate oraz FortiSwitch (model przykładowy: FS-TRAN-SFP+LR) - 30 szt.

IX. 10GBASE-SR SFP+ 850nm 300m DOM LC MMF Transceiver Module Wkładki światłowodowe do FortiGate oraz FortiSwitch (model przykładowy: FS-TRAN-SFP+SR) - 2 szt.

IP

X. Kable światłowodowe duplex typ LC MMF 1.5m (model przykładowy: Patchcord FX) - 10 szt.

XI. Kable światłowodowe duplex typ LC MMF 0.5m (model przykładowy: Patchcord FX) - 10 szt.

XII. Kable miedziane kat.6a 1m (model przykładowy: Patchcord S/FTP) - 10 szt.

XIII. Kable miedziane kat. 8 a 0.5m (model przykładowy: Patchcord S/FTP) -10 szt.

XIV. Prace wdrożeniowe

1) Audyt bieżącej konfiguracji,
2) przygotowanie koncepcji wdrożenia i migracji usług wraz z Zamawiającym,
3) montaż i instalacja urządzeń w siedzibie oraz w szafach rackowych należących do Zamawiającego,
4) konfiguracja nowego rozwiązania z zachowaniem ciągłości działania obecnej infrastruktury klienta,
5) testy konfiguracji i funkcjonalne,
6) przełączenie usług na nową infrastrukturę,
7) dokumentacja powykonawcza obejmująca opis podstawowych parametrów dostarczonego rozwiązania,
8) szkolenie z obsługi i konfiguracji wdrożonych urządzeń,
9) prace będą prowadzone w dni robocze w godzinach 7-16 w lokalizacji w Warszawie w siedzibie klienta,
10) Modernizacja infrastruktury sieciowej LAN – obejmuje projekt, wdrożenie, szkolenie oraz dokumentację (minimalna ilość godzin uwzględnionych w ofercie przeznaczonych na prace to 300h).

XV. WARUNKI REALIZACJI ZAMÓWIENIA

Zamawiający wymaga, aby Wykonawca w zakresie realizacji zamówienia:

1) dostarczył na własny koszt i ryzyko przedmiot zamówienia do siedziby Instytutu Technicznego Wojsk Lotniczych, ul. Księcia Bolesława 6, 01-494 Warszawa i przeprowadził rozładunek przedmiotu zamówienia w miejscu wskazanym przez Zamawiającego,
2) dostarczył cały przedmiot zamówienia fabrycznie nowy, nieużywany oraz pochodzący z bieżącej produkcji.
3) dostarczył wraz z przedmiotem zamówienia instrukcje obsługi w języku polskim lub angielskim,
4) dostarczył, wraz z przedmiotem zamówienia, dokument gwarancyjny w języku polskim lub angielskim, dla każdego produktu osobno.
5) przeprowadził wdrożenie, konfigurację dostarczonego przedmiotu zamówienia oraz szkolenie administratorów.

XVI. WARUNKI PRAC WDROŻENIOWYCH

Zamawiający wymaga, aby Wykonawca w ramach prac wdrożeniowych wykonał:

1) audyt bieżącej konfiguracji,
2) przygotowanie koncepcji wdrożenia i migracji usług wraz z Zamawiającym,
3) montaż i instalacja urządzeń w siedzibie oraz w szafach rackowych należących do Zamawiającego,
4) konfiguracje nowego rozwiązania z zachowaniem ciągłości działania obecnej infrastruktury klienta,

5) testy konfiguracji i funkcjonalne,
6) przełączenie usług na nową infrastrukturę,
7) dokumentacja powykonawcza obejmująca opis podstawowych parametrów dostarczonego rozwiązania,
8) szkolenie z obsługi i konfiguracji wdrożonych urządzeń,
9) prace będą prowadzone w dni robocze w godzinach 7-16 w lokalizacji w Warszawie w siedzibie klienta,
10) modernizacja infrastruktury sieciowej LAN etap 2 obejmuje projekt, wdrożenie, szkolenie oraz dokumentacja (minimalna ilość godzin zawartych w ofercie przeznaczonych na prace to 300h).

XVII. WARUNKI GWARANCJI SERWISOWEJ

Zamawiający wymaga, aby Wykonawca w ramach gwarancji serwisowej zapewnił:

1) świadczenie gwarancji serwisowej na okres 60 miesięcy,
2) świadczenie serwisu gwarancyjnego przez podmiot serwisujący który posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych,
3) dostarczenie licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów zawierających: Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analizy typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy,
4) naprawę lub wymianę urządzenia w przypadku jego wadliwości oraz dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7,
5) rozszerzone wsparcie techniczne dla systemu gwarantujące dostawę sprzętu zastępczego do czasu usunięcia awarii 24x7xNBD tj. udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu od momentu potwierdzenia zasadności zgłoszenia, realizowane przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres trwania serwisu gwarancyjnego,
6) przyjmowanie zgłoszeń serwisowych w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim w trybie 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina, reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym,
7) przeglądy serwisowe przedmiotu zamówienia, jeśli takie są niezbędne dla prawidłowego działania przedmiotu zamówienia i/lub dla utrzymania obsługi gwarancyjnej.

XVIII. TERMIN REALIZACJI - Termin realizacji zamówienia: do 180 dni od daty zawarcia umowy.