

Załącznik nr 1 do Zapytania ofertowego  
Załącznik nr 1 do Umowy nr RU ...../2022

## OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest „**Zakup, dostawa sprzętu komputerowego na potrzeby Centrum Edukacji Artystycznej**”
2. W ramach przedmiotu zamówienia Wykonawca zobowiązuje się dostarczyć na własny koszt Zamawiającemu do jego siedziby tj. ul Mikołaja Kopernika 36/40 , 00-924 Warszawa (IV piętro pok. 409) niżej wymieniony sprzęt elektroniczny:
3. Parametry techniczne sprzętu elektronicznego i wymagania Zamawiającego:

### **Pakiet I: zintegrowany system bezpieczeństwa UTM Fortinet FortiGate 100F**

#### Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

#### Redundancja, monitoring i wykrywanie awarii

- 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.
- W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
- Monitoring stanu realizowanych połączeń VPN.
- System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

#### Interfejsy, Dysk, Zasilanie:

- System realizujący funkcję Firewall musi dysponować minimum:
  - 16 portami Gigabit Ethernet RJ-45.
  - 8 gniazdami SFP 1 Gbps.
  - 2 gniazdami SFP+ 10 Gbps.
- System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające połączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- System musi być wyposażony w zasilanie AC.

#### Parametry wydajnościowe:

- W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 56 tys. nowych połączeń na sekundę.
- Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
- Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
- Wydajność szyfrowania IPsec VPN nie mniej niż 10 Gbps.
- 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.
- 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
- 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

#### Funkcje Systemu Bezpieczeństwa:

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

- Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
- Kontrola Aplikacji.
- Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN.
- Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
- Ochrona przed atakami - Intrusion Prevention System.
- Kontrola stron WWW.
- Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
- Zarządzanie pasmem (QoS, Traffic shaping).
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
- Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
- Analiza ruchu szyfrowanego protokołem SSL.
- Analiza ruchu szyfrowanego protokołem SSH.

### Polityki, Firewall

- Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
  - Translację jeden do jeden oraz jeden do wielu.
  - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
- W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
  - Amazon Web Services (AWS).
  - Microsoft Azure
  - Cisco ACI.
  - Google Cloud Platform (GCP).
  - OpenStack.
  - VMware vCenter (ESXi).

### Połączenia VPN

- System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
  - Wsparcie dla IKE v1 oraz v2.
  - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
  - Obsługa protokołu Diffie-Hellman grup 19 i 20.
  - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
  - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
  - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
  - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
  - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
  - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
- System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
  - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
  - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
  - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwi realizację połączeń IPSec VPN lub SSL VPN.

### Routing i obsługa łączy WAN

- W zakresie routingu rozwiązanie powinno zapewniać obsługę:
  - Routingu statycznego.
  - Policy Based Routingu.

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

#### Zarządzanie pasmem

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

#### Ochrona przed malware

- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
- System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
- 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.
- System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

#### Ochrona przed atakami

- Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
- Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- System musi dysponować sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.
- 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.
- Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

#### Kontrola aplikacji

- Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

- Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

#### Kontrola WWW

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

#### Uwierzytelnianie użytkowników w ramach sesji

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

#### Zarządzanie

- 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.
- Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
- System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
- System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

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

#### Logowanie

- 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.
- 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.
- Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
- Musi istnieć możliwość logowania do serwera SYSLOG.

#### Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

#### Serwisy i licencje

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

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Sygnatury ochrony systemów przemysłowych SCADA na okres 36 miesięcy

#### Gwarancja oraz wsparcie

- Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

#### Opisy do wymagań ogólnych

- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.



## PAKIET II

Wewnętrzny punkt dostępowy: FortiAP-231F-E w zestawie z AC Power adapter.

Parametry minimum:

Trzy anteny radiowe

Dwa porty Ethernet

Anteny: 3 wewnętrzne WiFi + 1 BLE/ZigBee

Dostęp w pasmach 2,4 i 5 GHz

Jedna antena Bluetooth

Funkcje: Orthogonal Frequency Division Multiple Access (OFDMA), MU-MIMO

Wsparcie techniczne FortiCare Premium: 3 lata

AC Power adapter: SP-FAP200-PA-EU

4. Dostarczone urządzenia muszą być fabrycznie nowe, nieużywane, bez wad i uszkodzeń, pochodzić z bieżącej produkcji.

5. Oferowany sprzęt musi spełniać parametry techniczne i jakościowe określone w pkt 3 (Zamawiający nie dopuszcza osiągnięcia określonych/wymaganych funkcjonalności/portów przy użyciu przejściówek/ adapterów).

6. Zamawiający dopuszcza składanie ofert częściowych.

7. Z wyłonionym Wykonawcą, Zamawiający podpisze umowę na zakup i dostawę sprzętu komputerowego.