

Miasto Brańsk
ul. Rynek 8
17-120 Brańsk
NIP: 543-20-69-834
tel. 85/7375005
e-mail: sekretariat@bransk.um.gov.pl
adres strony internetowej: <http://bip.um.bransk.wrotapodlasia.pl>

Brańsk, dnia 02.06.2022 r.

znak sprawy: GKM.271.3.2022

ZAPYTANIE OFERTOWE

Zakup sprzętu i oprogramowania w ramach Programu Operacyjnego Polska Cyfrowa na lata 201-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-00-001/21-00.

Zamawiający: Miasto Brańsk

zaprasza do złożenia oferty na:

I. Część zamówienia:

1. Dostawa 1szt. serwer o parametrach nie gorszych niż:

Procesor lub procesory: 16 rdzeni
Pamięć RAM: 48 GB
Przestrzeń dyskowa: 1 TB (RAW) na szybkich dyskach NVMe/SSD
Przystosowany do montażu w szafie rackowej
Szyny do montażu w szafie rackowej
Gwarancja producenta na 1 rok z wyłączeniem dysków
Gwarancja producenta dysków 2 lata.

2. Dostawa 15 szt. Tabletów o parametrach nie gorszych niż:

Liczba rdzeni – 8
Przekątna ekranu – 10 cali
Rozdzielczość ekranu – 1280x800 pikseli
Funkcje ekranu – Autoobrót, Dotykowy, Multi-Touch
Pamięć wbudowana – 64GB
Pamięć RAM – 4GB
Pojemność akumulatora – 5000mAh
Komunikacja – modem, gniazdo karty sim
WiFi – a/b/g/n

Transmisja danych – LTE
Oprogramowanie – Android 10
Gwarancja producenta 1 rok.

3. Dostawa 1szt. NAS o parametrach nie gorszych niż:

Procesor AMD Ryzen™ Embedded V1500B 4-core/8-thread 2.2 GHz procesor
Pamięć DDR4 SODIMM o pojemności 4 GB (do 64 GB 2x32GB)
Support ECC memory
2x port 2,5GbE
port PCIe Gen3 x 8
2x M.2 PCIe Gen3
Wnęki dla 8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s
Kompatybilność dysków 3,5-calowe dyski twarde SATA, 2,5-calowe dyski twarde SATA,
2,5-calowe dyski SSD SATA
Port USB 3.2 Gen 2 (10 Gb/s) - 4 (2 x Type A, 2 x Type C)
Obudowa rackowa do montażu w szafie teleinformatycznej.

4. Dostawa 1szt. SWITCH o parametrach nie gorszych niż:

Typ przełącznika – Zarządzany
Przełącznik wielowarstwowy - L2/L3
Podstawowe przełączanie RJ-45 Liczba portów Ethernet - 16
Ilość portów Gigabit Ethernet - 16
Liczba portów SFP Combo – 2
Liczba portów USB 2.0 - 1
Podstawowe przełączania Ethernet RJ-45 porty typ Gigabit Ethernet (10/100/1000)
Obsługa jakości serwisu (QoS)
Zarządzanie przez stronę www
Raport zdarzeń systemowych
Standardy komunikacyjne: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.1s, IEEE
802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3af, IEEE
802.3at, IEEE 802.3az, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z
Technologia okablowania Copper Ethernet 10BASE-T, 10GBASE-T, 100BASE-
TX, 1000BASE-T
Dublowanie portów
Agregator połączenia
Kontrola wzrostu natężenia ruchu
Limit częstotliwości
Protokół drzewa rozpinającego
Blokowanie head-of-line (HOL)
Obsługa sieci VLAN
Funkcje wirtualnej sieci LAN Stacked VLAN, Voice VLAN, Protocol-based VLAN
Liczba VLANs - 255
Przepustowość routowania/przełączania - 36 Gbit/s
Prędkość przekazywania - 26,78 Mpps
Wielkość tabeli adresów – 8000
Liczba kolejek – 8
Zgodny z Jumbo Frames
Rozszerzenie Jumbo Frames - 9000

Pamięci bufora pakietów - 12 MB
Funkcje DHCP: DHCP server, DHCP relay
Lista kontrolna dostępu (ACL)
Zasady Listy Kontroli Dostępu (ACL) – 512
IGMP snooping
Szyfrowanie / bezpieczeństwo: 802.1x RADIUS,HTTPS,SSH,SSL/TLS
Zabezpieczenie przed wejściem w pętlę
Zapobieganie atakom DoS
Algorytm planowania kolejki - Weighted Round Robin (WRR)
Protokół rejestracji GARP VLAN (GVRP)
Taktowanie procesora - 800 Mhz
Pojemność pamięci wewnętrznej - 512 MB
Wielkość pamięci flash - 256 MB

5. Dostawa 3 szt. AccessPoints o parametrach nie gorszych niż:

Szybkość przesyłania danych: 3000 Mbit/s,
Maksymalna szybkość przesyłania danych (2.4 GHz): 600 Mbit/s,
Maksymalna szybkość przesyłania danych (5 GHz): 2400 Mbit/s.
Szyfrowanie / bezpieczeństwo: WPA,WPA-Enterprise,WPA-PSK,WPA2,WPA3.
Obsługiwane protokoły sieciowe: 802.11ax, 802.11ac, 802.11n, 802.11g, 802.11b, 802.11a, 802.3at, 802.1Q.
Power over Ethernet (PoE)
Napięcie: 44 - 57 V,
Maksymalne zużycie mocy: 16,5 W.
Umieszczenie: Sufit, Ściana
Liczba osób mogących korzystać z produktu. Liczba użytkowników – 300
MIMO - Multi User MIMO
Obsługa sieci VLAN
Obsługa jakości serwisu (QoS)
Stopień ochrony IP – IP54
Przycisk reset
Certyfikaty - CE, FCC, IC
Antena wewnętrzna
Poziom wzmocnienia anteny - 5,5 dBi
Taktowanie procesora - 1,35 Mhz
Zakres temperatur (eksploatacja): -30 - 60 °C
Zestaw do montażu

6. Dostawa 2 szt. Monitorów o parametrach nie gorszych niż:

Przekątna ekranu - 32 cale / 80 cm / 16:9, VA LED
Zakrzywiony ekran
Rozdzielczość - 2560 x 1440
Kontrast statyczny / dynamiczny - 3000 :1 / 3000000 :1
Jasność ekranu - 250 cd/m2
Czas reakcji matrycy - 4 ms
Wielkość plamki - 0,274 mm
Kąt widzenia w pionie / w poziomie - 178 stopni / 178 stopni
Liczba wyświetlanych kolorów - 16,7 mln

Częstotliwość odświeżania obrazu - 75 Hz
Złącza - DisplayPort x 1, HDMI x 1, wyjście liniowe audio
Możliwość montażu na ścianie - Standard VESA 100x100 mm
Regulacja pochylania w pionie, technologia AMD® FreeSync, zakrzywienie 1500R
Zużycie energii SDR - 37 kWh/1000h
Pobór mocy (tryb czuwania) - 0,5 W
Wyposażenie: instrukcja obsługi, kabel HDMI, kabel zasilający.

7. Dostawa 5 szt. Laptopów o parametrach nie gorszych niż:

Procesor: Core i7-1165G7, taktowanie rdzeni procesora 2,8 GHz, taktowanie trybu turbo 4,7 GHz, pamięć cache procesora 12 MB
Matryca: Przekątna matrycy 15,6 cali, rozdzielczość FullHD 1920x1080, matowa IPS, jasność 250nit
Pamięć RAM: 16GB, rozbudowa do 32GB, częstotliwość 3200MHz, SODIMM DDR4
Dysk: SSD, 512GB, M.2 (PCIe/NVMe 2242), wolny slot 1x M.2 (PCIe)
Karta graficzna: INTEL, Iris Xe Graphics
Komunikacja: karta sieciowa przewodowa 1000Mbps, bezprzewodowa WiFi 6 (802.11 ax)
Interfejsy: HDMI, USB 2.0 (480 Mbps), USB 3.2 Gen 1 (5 Gbps), Thunderbolt 4 (z Display Port), RJ45, Wyjście słuchawkowe Combo, Wejście mikrofonu Combo
Multimedia: Karta dźwiękowa HD Audio, Ilość głośników 2, Moc głośników 2 W, Wbudowana kamera 0,9 Mpix + IR, przesłona kamery, wbudowany mikrofon
Klawiatura: kład klawiatury Qwerty (International), Podświetlenie klawiatury, Panel numeryczny klawiatury, Odporność na zachłapanie klawiatury, Touchpad, Trackpoint
System operacyjny: Windows 11 Pro, 64 bit, Wersja językowa systemu operacyjnego polska
Akumulator: litowo-polimerowy 45Wh
Zabezpieczenia: Gniazdo linki zabezpieczającej, czytnik linii papilarnych, szyfrowanie TPM
Inne: wzmacniana konstrukcja
Rodzaj gwarancji - Carry-In/Door-To-Door (Naprawa w serwisie)

8. Dostawa 2 szt. Stacji dokujących dedykowanych do laptopów o w/w parametrach.

9. Dostawa 1 szt. Stacji Roboczej AiO o parametrach nie gorszych niż:

Procesor: Intel Core i5-10500T (6 rdzeni, 2.30 GHz do 3.80 GHz, 12 MB cache)
Chipset Intel Q570
Pamięć RAM: 16 GB (SO-DIMM DDR4, 2666 MHz)
Maksymalna obsługiwana ilość pamięci RAM 64 GB
Liczba gniazd pamięci (ogółem / wolne) 2/0
Typ ekranu: Matowy, LED, WVA
Przekątna ekranu: 23,8"
Rozdzielczość ekranu: 1920 x 1080 (FullHD)
Karta graficzna: Intel UHD Graphics 630
Wielkość pamięci karty graficznej: Pamięć współdzielona
Dysk SSD PCIe: 256 GB
Dźwięk: Wbudowane dwa mikrofony, zintegrowana karta dźwiękowa, wbudowane głośniki stereo
Kamera internetowa: 2.1 Mpix
Łączność: Wi-Fi 6 (802.11 a/b/g/n/ac/ax), LAN 10/100/1000 Mbps, Bluetooth

Złącza - panel tylny: USB 2.0 - 2 szt., USB 3.2 Gen. 2 - 2 szt., Wyjście słuchawkowe/głośnikowe - 1 szt., RJ-45 (LAN) - 1 szt., Display Port - 1 szt., AC-in (wejście zasilania) - 1 szt.

Złącza - panel boczny: USB 3.2 Gen. 1 - 1 szt., USB Type-C - 1 szt., Wyjście słuchawkowe/wejście mikrofonowe - 1 szt., Czytnik kart pamięci - 1 szt.

Inne: Możliwość zabezpieczenia linką (port Kensington Lock), wbudowany moduł TPM, kamera z wbudowaną zaślepką, mysz i klawiatura w zestawie, klawiatura bezprzewodowa, mysz bezprzewodowa,

System operacyjny: Microsoft Windows 11 Pro,

Dołączone oprogramowanie: Partycja recovery (opcja przywrócenia systemu z dysku).

Klauzule gwarancje

Software

Wszystkie Produkty wymienione w niniejszym opisie muszą pochodzić bezpośrednio od producenta lub z oficjalnych i autoryzowanych przez Producenta kanałów dystrybucyjnych. Zamawiający wymaga, aby Wykonawca posiadał kwalifikacje i uprawnienia wymagane do prawidłowej realizacji przedmiotu zamówienia. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy komputerami (np. w przypadku wymiany sprzętu). Gwarancja dostępności najnowszej wersji oprogramowania oraz bieżące jego poprawki i uaktualnienia w trakcie trwania umowy. Zamawiający dopuszcza oferowanie produktów o szerszej niż opisana funkcjonalności.

W ramach procedury odbiorczej Wykonawca w terminie do 14 dni roboczych od dnia zawarcia umowy zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym ze strony Zamawiającego osobom na:

- a) pobieranie oprogramowania.
- b) pobieranie kluczy aktywacyjnych do oprogramowania.
- c) sprawdzanie liczby zakupionych licencji w wykazie oprogramowania.

Potwierdzeniem odbioru dostawy licencji będzie podpisany przez Wykonawcę i Zamawiającego protokół odbioru.

Hardware

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania

II . Część zamówienia:

1. Przedmiotem zamówienia jest dostawa licencji Microsoft:

1. Office 2021 dla Użytkowników Domowych i Małych Firm – 6 szt.
2. Windows Server Standard 2019 16 Core Polish – 1 szt.
3. Licencje CAL na użytkownika Windows Server 2019 AD (Active Directory) – 24 szt.
4. Licencje CAL na użytkownika Windows Server 2019 RDS (Remote Desktop Services Client Access License) – 5 szt.

Klauzule gwarancje

Software

Wszystkie Produkty wymienione w niniejszym opisie muszą pochodzić bezpośrednio od producenta lub z oficjalnych i autoryzowanych przez Producenta kanałów dystrybucyjnych. Zamawiający wymaga, aby Wykonawca posiadał kwalifikacje i uprawnienia wymagane do prawidłowej realizacji przedmiotu zamówienia. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy komputerami (np. w przypadku wymiany sprzętu). Gwarancja dostępności najnowszej wersji oprogramowania oraz bieżące jego poprawki i uaktualnienia w trakcie trwania umowy. Zamawiający dopuszcza oferowanie produktów o szerszej niż opisana funkcjonalności. Gwarancja dostępności najnowszej wersji oprogramowania oraz bieżące jego poprawki i uaktualnienia w trakcie trwania umowy. Licencje muszą być nowe, wcześniej nieaktywowane.

W ramach procedury odbiorczej Wykonawca w terminie do 14 dni roboczych od dnia zawarcia umowy zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym ze strony Zamawiającego osobom na:

- a) pobieranie oprogramowania.
- b) pobieranie kluczy aktywacyjnych do oprogramowania.
- c) sprawdzanie liczby zakupionych licencji w wykazie oprogramowania.

Potwierdzeniem odbioru dostawy licencji będzie podpisany przez Wykonawcę i Zamawiającego protokół odbioru.

Gwarancja dostępności najnowszej wersji oprogramowania oraz bieżące jego poprawki i uaktualnienia w trakcie trwania umowy.
Licencje muszą być nowe, wcześniej nieaktywowane.

III . Część zamówienia:

Dostawa 1 szt. Fierewall/ UTM o parametrach nie gorszych niż:

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'a, 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:

- Firewall.
- Ochrony w warstwie aplikacji.

- 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 sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

3. Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
 - 10 portami Gigabit Ethernet RJ-45.
 - 2 gniazdami 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'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 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 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

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 - zaporą ogniową 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. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. 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:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
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.
 - Amazon Web Services (AWS).
 - Microsoft Azure
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware NSX.

7. Połączenia VPN.

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19 i 20.

- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - 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:
- Routingu statycznego.
 - Policy Based Routing.
 - 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 laboratorium 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, Dynamic 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:
 - Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasel 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:

- 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: 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 12 miesięcy.

20. Gwarancja oraz wsparcie.

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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. Opisy do wymagań ogólnych.

- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem

niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

- 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.
1. Zamawiający dopuszcza składanie ofert częściowych zgodnie z podziałem określonym w Zapytaniu ofertowym. Wykonawca może złożyć ofertę na dowolną ilość części zamówienia.
 2. Termin realizacji zamówienia: 14 dni dla dostawy urządzeń od daty podpisania umowy. Za termin wykonania przedmiotu zamówienia uważa się datę podpisania protokołu odbioru końcowego przedmiotu zamówienia.
 3. Wykonawca nie może być powiązany z Zamawiającym osobowo ani kapitałowo (Załącznik Nr 2 Oświadczenie o braku powiązań kapitałowych i osobowych z Zamawiającym należy dołączyć do oferty).
 4. Kryteria oceny ofert:
Cena – waga – 100%
W przypadku wpływu kilku ofert o tej samej liczbie punktów, Zamawiający zastrzega sobie prawo do wystąpienia do Wykonawców, których dotyczyć będzie taka sytuacja, o przedstawienie ofert dodatkowych.
 5. Miejsce i termin złożenia oferty: **09.06.2022, godzina 12.00.**
Oferty można przesłać pocztą na adres poczty elektronicznej: sekretariat@bransk.um.gov.pl lub złożyć w siedzibie zamawiającego tj. Urządzie Miasta Brańsk, ul. Rynek 8, 17-120 Brańsk (Sekretariat). Oferty złożone po terminie bądź w inny sposób nie będą rozpatrywane.
 6. Termin otwarcia ofert: **09.06.2022 godzina 13.00**
 7. Warunki płatności: przelew 14 dni od momentu dostarczenia prawidłowo wystawionej faktury.
 8. Osoba upoważniona do kontaktu z Wykonawcami: Joanna Półtorak, e-mail: jpoltorak@bransk.um.gov.pl; Radosław Hofman (informatyk), e-mail: radek@hofman.eu.org

9. Sposób przygotowania oferty: ofertę należy sporządzić w formie pisemnej (elektronicznej), w języku polskim. Wykonawca składając ofertę jest zobowiązany dołączyć do niej następujące dokumenty:

- 1) Załącznik Nr 1 Oferta;
- 2) Załącznik nr 2 Oświadczenie o braku powiązań kapitałowych i osobowych z Zamawiającym
- 3) Załącznik Nr 3 Projekt umowy.

10. W przypadku nie dołączenia do oferty wymaganych dokumentów oferta zostanie odrzucona z przyczyn formalnych.

11. Sposób rozliczeń: wszelkie rozliczenia związane z realizacją niniejszego zamówienia dokonywane będą w PLN.

12. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

- a) administratorem Pani/Pana danych osobowych jest Miasto Brańsk, ul. Rynek 8, 17-120 Brańsk NIP 543-20-69-834; REGON 050658947;
- b) inspektorem ochrony danych osobowych w gminie Mieście Brańsk jest Pan R. Andrzejewski, e-mail: iod.r.andrzejewski@szkoleniaprawnicze.com.pl, tel. 504 976 690;
- c) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego, o którym mowa w rozdziale 3;
- d) Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 ustawy;
- e) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
- f) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencja niepodania określonych danych wynikają z ustawy;
- g) w odniesieniu do Pani/pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
- h) posiada Pani/Pan:
 - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników);
 - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa

w art. 18 ust. 2 RODO (prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego;

- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- i) nie przysługuje Pani/Panu:
- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - prawo do przenoszenia danych osobowych, o których mowa w art. 20 RODO;
 - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.
- j) Skorzystanie przez osobę, której dane osobowe dotyczą, z uprawnienia do sprostowania lub uzupełnienia, o którym mowa w art. 16 rozporządzenia 2016/679, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą.
- k) Zgłoszenie żądania ograniczenia przetwarzania, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, nie ogranicza przetwarzania danych osobowych do czasu zakończenia tego postępowania.

BURMISTRZ

Eugeniusz Tomasz Koczewski