Załącznik nr 2 do zapytania ofertowego

ZP. 271.7.2023

Szczegółowy Opis Przedmiotu Zamówienia

dot. Zapytania ofertowego na „Zakup wraz z dostawą sprzętu komputerowego, oprogramowania oraz przeprowadzenie szkolenia dla pracowników" w ramach projektu „Cyfrowa Gmina" realizowanego przez Gminę Nagłowice w ramach Umowy o powierzenie grantu o numerze 4360/2/2022 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 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.05.01.00-00-0001/21-00.

Spis treści

Część I

1) Serwer wraz oprogramowaniem serwerowym – 1 szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1	**Obudowa**	Urządzenie fabrycznie nowe. Obudowa Rack o wysokości max 2U z możliwością instalacji do 16 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
2	**Płyta główna**	Płyta główna z możliwością zainstalowania minimum dwóch procesorów Intel 3rd Gen. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
4	**Procesor**	Zainstalowany jeden procesor 16-rdzeniowy, min. 2.4 GHz (Turbo Speed min. 3.4 GHz), klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 29000 w teście Passmark CPU Mark dostępnym na stronie https://www.cpubenchmark.net/.
5	**RAM**	64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
6	**Zabezpieczenia pamięci RAM**	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
7	**Gniazda PCI**	minimum dwa sloty PCIe z czego przynajmniej jeden generacji 4
8	**Interfejsy sieciowe/FC/SAS**	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT

9	**Dyski twarde**	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 4 dyski SAS o pojemności min. 1.2TB, 12Gbps, 10k Hot-Plug Zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. W przypadku awarii dyski twarde pozostają własnością Zamawiającego
10	**Kontroler RAID**	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
11	**System operacyjny**	Windows Server 2022 Standard 25x licencja Windows Server 2022 User CALs
12	**Wbudowane porty**	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
13	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
14	**Zasilacze**	2 Redundantne, Hot-Plug min. 750W każdy
15	**Bezpieczeństwo**	– zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych; – wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą; – moduł TPM 2.0
16	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

		– zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); – szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; – wsparcie dla IPv6 i NTP; – wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; – integracja z Active Directory; – możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; – wsparcie dla dynamic DNS; – wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. – możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
17	**Certyfikaty**	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
18	**Warunki gwarancji**	3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
19	**Dokumentacja użytkownika**	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

2) Serwer NAS – 2 szt.

Minimalne wymagania i parametry techniczne urządzenia:

1. Urządzenie fabrycznie nowe.
2. Funkcje: wsparcie dla wirtualizacji, scentralizowana pamięć masowa na dane, backup, udostępnianie i przywracanie systemu po awarii.
3. Obudowa: typu Tower
4. Procesor posiadający minimum 4 rdzenie oraz 8 wątków; architektura 64 bit. Umożliwiający osiągnięcie przez procesor wyniku powyżej 5250 pkt w teście Passmark CPU Mark (https://www.cpubenchmark.net/mid_range_cpus.html)
5. Pamięć RAM: 8 GB z możliwością rozbudowy
6. Rodzaj pamięci: SODIMM DDR4
7. Pamięć flasch – 5 GB
8. Możliwość zainstalowania łącznie 4 dysków 2,5" lub 3,5"
9. Zainstalowane dyski: min. 2 dysków HDD SATA po 4TB każdy o prędkości min 5400 obr/min przeznaczone do pracy z urządzeniami NAS z możliwością wymiany podczas pracy (hot-swap)
10. Poziom RAID: 0, 1, 5, 6.
11. Architektura sieci : GigabitEthernet
12. Interfejs sieciowy: 2 x 10/100/1000/2500 Mbit/s
13. Gniazda we/wy: 2 x RJ-45 LAN
14. Gniazda we/wy: 3 x USB 3.0
15. Gniazda we/wy: 1 x USB 3.1
16. Gniazda rozszerzeń: 2 x PCIe 3.0 x 4
17. Zasilanie: 250W, 100-240V AC, 50-60Hz, 3.5A
18. Funkcje: zainstalowane na urządzeniu oprogramowanie dedykowane przez producenta urządzenia do tworzenia kopii zapasowych dostępne także przez przeglądarkę www przy wykorzystaniu bezpiecznego protokołu transmisji danych (co najmniej ssh); obsługa maszyn wirtualnych VMware / Hyper-V; możliwość tworzenia połączeń sieciowych, uwierzytelnienie użytkowników Active Directory.
19. Wykonawca udzieli instrukcji, potrzebnych wskazówek Zamawiającemu (przez kontakt telefoniczny lub zdalne połączenie) co do instalacji, integracji urządzenia z posiadanym przez

Zamawiającego systemem informatycznym i odpowiedniej konfiguracji potrzebnej do prawidłowej pracy w sieci Zamawiającego.

20. Gwarancja producenta: min. 24 miesiące gwarancji realizowanej w miejscu instalacji sprzętu, z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia. Gwarancja musi obejmować także dyski. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.

3) Stacje robocze typu All in One wraz z oprogramowaniem biurowym Microsoft Office -5 szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.	**Typ**	Komputer stacjonarny typu All in One, komputer fabrycznie nowy wbudowany w obudowę monitora.
2.	**Zastosowanie**	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
3.	**Procesor**	4-rdzeniowy, 8-wątkowy, osiągający w teście Passmark CPU Mark średni wynik przynajmniej 8750. PassMark - CPU Benchmarks - List of Benchmarked CPUs
4.	**Pamięć RAM**	8 GB DDR4 3200 MHz z możliwością rozbudowy. 1 wolny bank pamięci pozwalający na dalszą rozbudowę.
5.	**Dysk twardy**	500 GB w technologii SSD PCI-Express lub większy
6.	**Rozdzielczość ekranu**	1920 x 1080 pikseli
7.	**Karta Grafiki:**	- Zintegrowana z procesorem
8.	**Karta dźwiękowa**	- Zintegrowana z płytą główną, zgodna z High Definition Audio.
9.	**Karta sieciowa**	- Interfejs wbudowany w płytę główną. - minimum 1 x 10/100/1000 Mbps (RJ-45, Gigabit Ethernet).
10.	**Karta sieci bezprzewodowej**	- Interfejs wbudowany w płytę główną lub na złączu PCI-Express lub USB - minimum w standardzie 802.11 b/g/ac
11.	**Obudowa**	Typu AIO, wyświetlacz od 23” wzwyż LCD w technologii LED, o formacie obrazu 16:9, Full HD, wbudowane, głośniki, mikrofon, matowa matryca, rozdzielczość ekran -1920 x 1080 pikseli
12.	**Złącza**	1 szt. – HDMI 2szt. – USB 2.0 2 szt. – USB 3.0 Złącze COMBO
13.	**Zasilanie**	Zasilacz zewnętrzny lub wbudowany
14.	**Klawiatura**	Klawiatura USB w układzie QWERTY

		Długość przewodu minimum 1,8m.
15.	**Mysz**	Mysz optyczna USB, 1200dpi, z dwoma przyciskami oraz rolką (scroll). Długość przewodu minimum 1,8m, podkładka pod mysz.
16.	**System operacyjny**	Dostarczane przez Wykonawcę komputery muszą posiadać zainstalowany 64 bitowy system operacyjny Microsoft Windows 11 w wersji PRO w polskiej wersji językowej.
17.	**Oprogramowanie biurowe**	Pakiet biurowy z licencją bezterminową: min. Microsoft Office Home & Bussines 2021 wersja obejmująca edytor tekstu, arkusz kalkulacyjny, program pocztowy, program do tworzenia prezentacji
18.	**Gwarancja i serwis**	Gwarancja 3 lata Door-To-Door

4) Laptopy wraz z oprogramowaniem biurowym Microsoft Office - 5 szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.	**Typ**	Komputer fabrycznie nowy typu notebook z ekranem o przekątnej 15,6”-18” i rozdzielczości nie mniejszej niż 1920 x 1080 pikseli (FullHD).
2.	**Procesor**	Procesor min. 4 rdzeniowy, pamięć cache 8MB, uzyskujący wynik średniej oceny co najmniej 10150 punktów w teście Passmark – CPU Mark według wyników procesorów publikowanych na stronie http://www.cpubenxchmark.net/cpu_list.php
3.	**Pamięć RAM**	DDR4 8 GB 3200 MHz z możliwością rozbudowy.
4.	**Dysk**	SSD 256GB M.2 PCI-Express lub większy
5.	**Karta graficzna**	Grafika zintegrowana
6.	**Multimedia**	Karta dźwiękowa zgodna z HD Audio. Wbudowane głośniki. Kamera HD.
7.	**Łączność**	Port 1Gbit LAN, wbudowane WiFi 802.11 a/b/g/n/ac
8.	**Bateria i zasilacz:**	Minimum 3 komorowa o pojemności 41Wh. Zasilacz dedykowany do notebooka.
9.	**Interfejsy WE/WY:**	1 szt. – HDMI 1x USB 2.0 Typ-A 2x USB 3.2 Gen 2 Typ-A 1x Thunderbolt™ 4, kompatybilne z USB Typ-C Wyjście słuchawkowe, mikrofonowe - COMBO

10.	**Układ klawiatury**	QWERTY
11.	**Certyfikaty i standardy:**	CE dla oferowanego komputera. ISO 9001:2015 dla autoryzowanego serwisu Producenta notebooka.
12.	**Bezpieczeństwo:**	Dedykowana dioda LED zintegrowanej kamery sygnalizująca pracę komponentu. Fizyczna przesłona na kamerze zintegrowana z obudową komputera. Zintegrowany moduł TPM
13.	**Warunki gwarancji:**	Gwarancja 3 lata Door-To-Door
14.	**Wymagana gwarancja na baterię**	Gwarancja 1 rok Door-To-Door
15.	**Wsparcie techniczne producenta:**	Możliwość sprawdzenia telefonicznego bezpośrednio u producenta oraz na stronie internetowej producenta oferowanego notebooka, po podaniu numeru seryjnego - konfiguracji sprzętowej notebooka oraz warunków gwarancji. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta notebooka, realizowany poprzez podanie na stronie internetowej producenta numeru seryjnego lub modelu notebooka
16.	**Oprogramowanie biurowe**	Dostarczane przez Wykonawcę komputery muszą posiadać zainstalowany pakiet biurowy z licencją bezterminową: min. Microsoft Office Standard 2021 wersja edukacyjna, obejmujący edytor tekstu, arkusz kalkulacyjny, program pocztowy, program do tworzenia prezentacji
17.	**Myszka**	Mysz optyczna USB, 1200dpi, z dwoma przyciskami oraz rolką (scroll). Długość przewodu minimum 1,8m, podkładka pod mysz.
18.	**System operacyjny**	Dostarczane przez Wykonawcę komputery muszą posiadać zainstalowany 64 bitowy system operacyjny Microsoft Windows 11 w wersji HOME lub PRO w polskiej wersji językowej.

Część II

1) Zakup i dostawa urządzenia typu UTM wraz ze wsparciem, licencją oraz pomocą techniczną na okres co najmniej 2 lat - 1 szt.

Wymagania Ogólne

Dostarczony system bezpieczeństwa powinien zawierać musi zapewniać wymienione poniżej funkcje bezpieczeństwa.

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

System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

Interfejsy:

1. System realizujący funkcję Firewall musi dysponować minimum:
   – 5 portami Gigabit Ethernet RJ-45;
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

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. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.
11. 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.
12. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
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

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 PATоraz:
    1) translację jeden do jeden oraz jeden do wielu;
    2) dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
    1) wsparcie dla IKE v1 oraz v2;
    2) obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM);
    3) obsługa protokołu Diffie-Hellman grup 19 i 20;
    4) wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE;
    5) tworzenie połączeń typu Site-to-Site oraz Client-to-Site;
    6) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności;

7) możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego;
8) obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth;
9) mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   1) 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.;
   2) pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta;
   3) producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

1) Routingu statycznego;
2) Policy Based Routingu;
3) protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

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.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System pozwala możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

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. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
4. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
5. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
6. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

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. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. 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.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
5. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

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.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu;
   - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP;
   - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. 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.

Logowanie

1. W ramach logowania system pełniący funkcję Firewall zapewnia 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.
2. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

Certyfikaty

1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA dla funkcji Firewall, IPS.

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: Kontrola Aplikacji, IPS, Antywirus, Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min. 24 miesięcy.

Instrukcje

Wykonawca w ramach zamówienia dostarczy Zamawiającemu instrukcje z funkcjonalności systemu w postaci plików PDF dot. poniższych tematów:

1) konfiguracja trybów pracy urządzenia (transparentny/sniffer lub router/NAT);
2) zarządzanie aktualizacjami;
3) budowa i optymalizacja reguł zapory sieciowej;
4) konfiguracja systemu wykrywania włamań ;
5) monitorowanie wykorzystania aplikacji i blokowanie malware/ransomware;
6) konfiguracja modułu filtrowania stron www;
7) konfiguracja profili antyspam;
8) zarządzanie wyciekiem danych DLP;
9) konfiguracja wielu łączy internetowych WAN;
10) raportowanie i analiza zdarzeń;
11) zaawansowana konfiguracja wielu łącz internetowych – SD WAN;
12) konfiguracja połączeń tunelowych Site-to-Site IPsec VPN;

13) zarządzanie dostępem zdalnym SSL- VPN w oparciu o dwu stopniowe metody uwierzytelniania;
14) instalacja i konfiguracja aplikacji dostępowej do VPN
15) zarządzanie mechanizmami routingu;
16) konfiguracja systemy ochrony przed atakami DDoS;
17) zaawansowana analiza logów i zdarzeń;
18) diagnostyka i rozwiązywanie problemów.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 24 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.

Rozszerzone wsparcie serwisowe

System powinien 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 min. 24 miesięcy.

Część III

1) Zakup i dostawa oprogramowania do zarządzania i monitorowania siecią - 1 szt.

Oprogramowanie typu Axence nVision®, moduł Network dla nielimitowanej liczby urządzeń oraz moduły Inventory, Users, DataGuard umożliwiające zarządzanie minimum 25 użytkownikami/komputerami lub równoważne.

Typ:
Oprogramowanie do zarządzania i monitorowania sieci.

Ogólny opis

1. **Minimalne wymagania funkcjonalne dla oprogramowania do zarządzania siecią i zasobami IT:**
   a) oprogramowanie musi składać się serwera zarządzającego, zdalnych konsoli oraz Agentów.
   b) komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2.
   c) oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.

d) dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów - nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników.
e) interfejs w jerzyku polskim.

2. Oprogramowanie posiada funkcjonalność monitorowania infrastruktury serwerowej i sieciowej w zakresie:

a) wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
b) wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
c) wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
d) serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
e) serwerów pocztowych: - monitorowanie serwisu odbierającego, jak i wysyłającego pocztę, - możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), - możliwość wykonywania operacji testowych, - możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa,
f) monitorowania serwerów WWW i adresów URL,
g) obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
h) obsługi komunikatów syslog i pułapek SNMP.
i) monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych- ruchu generowanego przez podłączone stacje robocze,
j) kontroli nad monitorem usług Windows,
k) monitorowania wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

3. Oprogramowanie umożliwia automatyczne gromadzenie danych o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie:

a) informacji dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.;
b) zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;
c) informacji o zainstalowanych aplikacjach oraz aktualizacjach Windows, umożliwiających audytowanie i weryfikację użytkowania licencji w organizacji;
d) informacji o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.;
e) możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera;

f) możliwość odczytania numeru seryjnego (klucze licencyjne);
g) możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;
h) możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.

4. Oprogramowanie posiada możliwość prowadzenia bazy ewidencji majątku IT w zakresie:

a) przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
b) definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz, możliwość importu danych z zewnętrznego źródła np. (.CSV);
c) generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania;
d) archiwizacji i porównywania audytów środków trwałych;
e) inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji dodatkowego oprogramowania poprzez manualne wykonanie skanów inwentaryzacji offline).

5. Oprogramowanie zapewnia funkcjonalność w zakresie monitorowania aktywności użytkowników na stacjach roboczych w zakresie:

a) faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy);
b) monitorowania procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika);
c) użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona);
d) informacji o edytowanych przez użytkownika dokumentach;
e) historii pracy (cykliczne zrzuty ekranowe);
f) listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
g) transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
h) wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument

był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek.

6. Oprogramowanie zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

a) skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie, archiwów ZIP;
b) zarządzanie posiadanymi licencjami;
c) audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji;
d) zarządzanie posiadanymi licencjami;
e) możliwość przypisania do programów numerów seryjnych, wartości itp.

7. Oprogramowanie zapewnia integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.

8. W zakresie pomocy technicznej system umożliwia:

a) tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów);
b) załączanie komentarzy, zrzutów ekranów i załączników w zgłoszeniach;
c) konfigurowanie pól niestandardowych, powiązanych w wybraną kategorią zgłoszenia;
d) przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach”);
e) dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę;
f) planowanie zastępstw w przydzielaniu zgłoszeń;
g) funkcję rozbudowanych raportów;
h) powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym;
i) baza zgłoszeń z rozbudowaną wyszukiwarką;
j) przejrzysty i intuicyjny interfejs webowy;
k) wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych;
l) komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu;
m) zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury;
n) dwukierunkowa wymiana plików;
o) zarządzanie procesami Windows z poziomu okna informacji o urządzeniu;
p) zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania);
q) procesowanie zgłoszeń z wiadomości e-mail;
r) integracja bazy użytkowników z Active Directory;

s) zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).

9. W zakresie kontroli dostępu do danych system umożliwia:

a) automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa;
b) ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych;
c) zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych;
d) integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania;
e) integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych;
f) możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB);
g) alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”);
h) zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami;
i) informacje o urządzeniach podłączonych do danego komputera;
j) lista wszystkich urządzeń podłączonych do komputerów w sieci;
k) audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych;
l) zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów użytkowników;
m) centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup użytkowników Active Directory.

10. Licencjonowanie:

Licencja wieczysta możliwość zwiększenia liczby zarządzanych stacji roboczych w ramach jednej licencji w dowolnym czasie. Nielimitowana liczba monitorowanych urządzeń sieciowych.

11. Opieka serwisowa:

12 miesięcy, aktualizacje, pomoc techniczna

12. Instalacja i wdrożeniowe dostarczonego oprogramowania:

1. Wykonawca udzieli wsparcia Zamawiającemu przy wdrożeniu i instalacji oprogramowania na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na 2 stanowiskach wskazanych przez Zamawiającego
2. Wsparcie przy instalacji i wdrożeniu odbywać się będzie w formie „zdalnego pulpitu”.

Część IV

1) Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa.

Wymagania ogólne dla szkolenia:

1. Szkolenie powinno odbywać się na terenie Gminy Nagłowice.
2. W ramach usługi zostanie przeszkolonych 30 osób w 2 grupach po 15 osób.
3. Szkolenie powinno trwać minimum 8 godzin szkoleniowych dla 1 grupy szkoleniowej
4. Zamawiający preferuje przeprowadzenie szkolenia w formie 4 godz. dziennie dla grupy.
5. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
6. Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
7. Szkolenia będą odbywać się w dni robocze w godzinach 8.00 – 16.00.
8. W przypadku szkoleń trwających do 4 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 4 godzin, organizowane będą dwie przerwy trwające 15 minut każda. Dodatkowo, w przypadku szkoleń trwających 8 godzin zaplanowana będzie przerwa trwająca 30 minut.
9. Szkolenia będą prowadzone w języku polskim.
10. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu i szczegółowego zakresu merytorycznego szkolenia, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 7 dni przed rozpoczęciem szkolenia.
11. W ramach organizacji szkoleń Wykonawca zapewni:
    1) Niezbędny sprzęt komputerowy do przeprowadzania szkolenia.
    2) Materiały szkoleniowe obejmujące szczegółowy zakres szkolenia oraz materiały merytoryczne zawierające szczegółowe informacje, które będą omawiane podczas szkolenia, które w formie elektronicznej przekaże uczestnikom szkolenia oraz Zamawiającemu w celach archiwalnych.
    3) Wydanie Uczestnikom szkolenia zaświadczeń/certyfikatów o ukończeniu szkolenia
    4) Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
    5) Prowadzenie dokumentacji szkolenia. Na dokumentację szkolenia składają się:
        a) Dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.
        b) Lista obecności uczestników szkolenia (dzienne, wypełniane oddzielnie każdego dnia szkolenia).
        c) Lista odbioru zaświadczeń o ukończeniu szkolenia.

12. W ramach organizacji szkolenia Zamawiający zapewni:
    1) Rekrutację osób biorących udział w szkoleniach.

2) Salę szkoleniową przystosowaną do prowadzenia zajęć dydaktycznych, zapewniającą warunki do przeprowadzenia szkolenia. Sala wyposażona będzie w wystarczającą liczbę miejsc.
3) Dostęp do sieci Internet.
4) Projektor multimedialny, nagłośnienie.
5) Odpowiednie warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne przepisami bezpieczeństwa i higieny pracy.

Tematyka szkolenia :

1. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
2. Polityka bezpieczeństwa w organizacji.
3. Definicja incydentu bezpieczeństwa i zasady postępowania z incydentem.
4. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
5. Ochrona danych osobowych w administracji publicznej.
6. Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko".
7. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
8. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
9. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
10. Prawidłowe korzystanie z oprogramowania antywirusowego.
11. Zasady aktualizacji programów i aplikacji.
12. Szyfrowanie dokumentów i poczty elektronicznej.
13. Polityka haseł, zarządzanie dostępem i tożsamością.

2) Szkolenie on-line dla administratora IT z zakresu konfiguracji UTM

Wymagania ogólne dla szkolenia:

1. Szkolenie on-line dla administratora IT z zakresu konfiguracji dostarczonego urządzenia klasy UTM.
2. Liczba osób: 1
3. Forma szkolenia: Szkolenie zdalne w godzinach 08:00 – 16:00;
4. Czas trwania szkolenia - 8 godzin – podzielone na 2 dni po 4 godziny;
5. Uczestnik po zakończeniu szkolenia otrzymuje zaświadczenie/certyfikat o ukończeniu szkolenia

Tematyka szkolenia:

- Konfiguracja trybów pracy urządzenia (transparentny/sniffer lub router/NAT)
- Zarządzanie aktualizacjami oraz backup
- Budowa i optymalizacja reguł zapory sieciowej

- Konfiguracja systemu wykrywania włamań (IDS/IPS)
- Monitorowanie wykorzystania aplikacji i blokowanie malware/ransomware
- Konfiguracja modułu filtrowania stron www
- Konfiguracja profili antyspam
- Zarządzanie wyciekiem danych DLP
- Konfiguracja wielu łączy internetowych WAN
- Raportowanie i analiza zdarzeń
- Zaawansowana konfiguracja wielu łącz internetowych – SD WAN
- Konfiguracja połączeń tunelowych Site-to-Site IPsec VPN
- Zarządzanie dostępem zdalnym SSL- VPN w oparciu o dwu stopniowe metody uwierzytelniania
- Instalacja i konfiguracja aplikacji Client VPN
- Zarządzanie mechanizmami routingu
- Konfiguracja systemy ochrony przed atakami DDoS
- Diagnostyka i rozwiązywanie problemów

Równoważność rozwiązań

Jeżeli wykonawca stwierdzi, że użyte w zapytaniu i w załącznikach parametry lub normy krajowe lub przenoszące na normy europejskie lub normy międzynarodowe mogą wskazywać na producentów produktów lub źródła ich pochodzenia to oznacza, że mają takie znaczenie, że parametry techniczne tak wskazanych produktów określają wymagane przez Zamawiającego minimalne oczekiwania co do jakości produktów, które mają być użyte do wykonania przedmiotu umowy. Wykonawca jest uprawniony do stosowania produktów równoważnych, przez które rozumie się takie, które posiadają parametry techniczne nie gorsze od tych wskazanych w zapytaniu i w załącznikach do zapytania. Na Wykonawcy spoczywa ciężar wskazania „równoważności".