Załącznik nr 1

Zmiana z dnia 28.09.2017 r.

Zakup, dostawa sprzętu biurowego i komputerowego z oprogramowaniem dla Urzędu Miejskiego w Świebodzicach

1) **Zakup komputerów- 10 sztuk**

DANE TECHNICZNE:

- Procesor – procesor wielordzeniowy minimum - 3,9 GHz, 3 MB pamięci podręcznej, 2 rdzenie lub równoważny
- Płyta główna Chipset Intel H270 lub równoważna
- Karta graficzna zintegrowana Intel HD Graphics 630 lub równoważna
- Gniazda rozszerzeń: 1 x PCIe 2.0 x 1 , 2 x PCIe 3.0 x 16, 1 x Turbo Drive (M.2 PCIe) dla karty WLAN
- Karta dźwiękowa
- Dysk HDD SATA 500 GB 7200 obr/min
- Napęd optyczny DVD-RW Super Multi l
- Pamięć RAM 8 GB DDR4 2400 MHz (1x8GB)
- System operacyjny Windows 10 Pro lub równoważny
- Obudowa Micro Tower
- Liczba portów USB – min. 8 szt. w tym USB 3.0 – min. 4 szt
- Porty wideo: minimum 1 x DisplayPort , minimum 1 x VGA (15 pin D-Sub)
- Interfejs sieciowy : 1 x 10/100/1000 Mbit/s
- wbudowany układ szyfrujący TMP
- EPEAT Gold
- Energy Star

2) **Zakup monitorów- 10 sztuk**

DANE TECHNICZNE:

- Jasność 250 cd/m²
- Czas reakcji 5 ms
- Kąt widzenia poziomy 178 °
- Kąt widzenia pionowy 178 °
- Plamka matrycy 0.248 mm
- Proporcje obrazu 16:9
- Przekątna ekranu 21.5"
- Technologia podświetlania Diody LED
- Kontrast statyczny 3000:1
- Kontrast dynamiczny 5 000 000:1
- Gniazda we/wy 1 x DisplayPort , 1 x 15-pin D-Sub
- Wbudowane głośniki
- Rozdzielczość FHD (1920 x 1080)

3) Zakup komputerów przenośnych – 3 sztuki

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Typ	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości: HD (1366x768) Non-Touch w technologii LED przeciwodblaskowy, jasność min 220 nitów, kontrast min 300:1
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Procesor	Procesor klasy x86, 2 rdzeniowy, niskonapięciowy, o TDP max 15W, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej 2,40 GHz, z pamięcią last level cache CPU co najmniej 3 MB lub równoważny 2 rdzeniowy procesor klasy x86 Zaoferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark wynik min.: 3820 punktów
Pamięć operacyjna RAM	4GB DDR4, możliwość rozbudowy do min 16GB
Parametry pamięci masowej	Min. 1TB SATA, możliwość instalacji dodatkowego dysku 2,5” lub modemu WWAN w wersji M.2 2280
Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 12, OpenGL 4.4, osiągająca w teście Average G3D Mark wynik na poziomie min.: 916 punktów
Wyposażenie multimedialne	Karta dźwiękowa stereo, wbudowane 2W głośniki stereo Wbudowana w obudowę matrycy kamera HD 720p wraz z dwoma mikrofonami Napęd optyczny DVD-RW
Wymagania dotyczące baterii i zasilania	3-cell, 48WHr, Li-Ion, Long-Life. Czas pracy na baterii wg dokumentacji producenta min 12 godzin Zasilacz o mocy min. 45W
System operacyjny	Zainstalowany 64-bitowy system operacyjny Microsoft Windows 10 Professional PL lub równoważny
Certyfikaty i standardy	– Certyfikat ISO9001:2000 lub równoważny dla producenta sprzętu – Certyfikat ISO 14001 lub równoważny dla producenta sprzętu – Deklaracja zgodności CE – Certyfikat EPEAT na poziomie GOLD dla Polski lub równoważny – Certyfikat EnergyStar v 6.1 lub równoważny
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 lub równoważną oraz wykazana zgodnie z normą ISO 9296 lub równoważną w pozycji operatora w trybie (IDLE) wynosząca maksymalnie 22 dB
Waga	maksymalnie 2,1 kg z baterią 3-cell
BIOS	Możliwość odczytania z BIOS: 1. Wersji BIOS wraz z datą wydania wersji 2. Modelu procesora, prędkości procesora, wielkość pamięci cache L1/L2/L3 3. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności, producencie i obsadzeniu na poszczególnych slotach 4. Informacji o dysku twardym: typ, producent, model 5. Informacji o napędzie optycznym: model (jeśli jest zainstalowany napęd optyczny) 6. Informacji o MAC adresie karty sieciowej Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, kontrolera audio, portów USB, czytnika kart SD, wewnętrznego głośnika, mikrofonu, karty dźwiękowej, funkcji TurboBoost, wirtualizacji, bluetooth z poziomu BIOS bez uruchamiania systemu

	operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie administratora. BIOS musi posiadać funkcję update BIOS z opcją automatycznego update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
Bezpieczeństwo	Złącze typu Kensington Lock lub równoważne TPM 2.0 1. BIOS musi posiadać możliwość - skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS, - możliwość ustawienia hasła na dysku (drive lock) - blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio; - blokady/wyłączenia poszczególnych kart rozszerzeń/slotów PCIe - kontroli sekwencji boot-ącej; - startu systemu z urządzenia USB - funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń 2. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2.0) lub równoważnym; 3. Możliwość zapięcia linki typu Kensington lub równoważnej i kłódki do dedykowanego oczka w obudowie komputera 4. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funcjonalności systemu diagnostycznego: - informacje o systemie, min.: 1. Procesor: typ procesora, jego obecna prędkość 2. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamieci, nr seryjny, typ pamieci, nr części, nazwa producenta 3. Dysk twardy: model, wersja firmware, nr seryjny, procentowe zużycie dysku 4. Napęd optyczny: model, wersja firmware, nr seryjny – jeśli jest zainstalowany 5. Bateria: nr seryjny, napięcie 5. Data wydania i wersja BIOS 6. Nr seryjny komputera - możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera - możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiekowej, klawiatury, myszy, sieci, płyty głównej, kamery internetowej, modułu wifi, portów USB, karty graficznej, baterii - rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii
Wymagania dodatkowe	1. Wbudowane porty i złącza: 1 x VGA, 1 x HDMI, 1 szt. USB 3.0, 2 szt. USB 2.0, 1 szt USB Typ-C, RJ-45, 1 x złącze słuchawkowe stereo/liniowe wyjście + złącze

	mikrofonowe (COMBO audio), czytnik kart multimedialnych SD/SDHC/SDXC, wbudowana kamera 720p w obudowę ekranu komputera + 2 mikrofony, napęd optyczny DVD-RW 2. Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną oraz WLAN 802.11 ac 2x2 nvP wraz z Bluetooth 4.2, zintegrowany z płytą główną lub w postaci wewnętrznego modułu. 3. Klawiatura (układ US -QWERTY) wraz z wydzieloną z prawej strony klawiaturą numeryczną odporna na zalanie. 4. Touchpad. 5. Czytnik linii papilarnych

4) Zakup serwera - 2 sztuki

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 4U RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie)
Procesor	jeden procesor co najmniej dziesięciordzeniowy, x86 - 64 bity, który zapewnia dla konfiguracji dwuprocesorowej wydajność w testach SPECfp_rate2006 wynik nie gorszy niż 706 punktów.
Pamięć operacyjna	Minimum 64GB RDIMM DDR4, z możliwością rozbudowy do minimum 3TB. Minimum 24 sloty na pamięć.
Sloty rozszerzeń	Możliwość rozbudowy serwera do minimum 5 slotów PCI-Express Generacji 3 pełnej wysokości (full height), w tym minimum trzy sloty x16 (prędkość slotu – bus width). Minimum 2 z gniazd PCI-Express x16 (bus width) mają umożliwiać instalację kart o pełnej wysokości i długości (Full-length / full height).
Dysk twardy	Zainstalowane minimum cztery dyski twarde 4 TB 12G SAS 10k. Obudowa serwera na 8 dysków LFF (3,5”) typu Hot Swap, SAS/SATA/SSD lub równoważna.
Dodatkowe urządzenia w zestawie	Napęd optyczny DVDRW
Kontroler	Wbudowany kontroler macierzowy SATA 12Gb z pamięcią cache 2GB, zapewniający obsługę min. 8 napędów dyskowych SATA oraz obsługujący poziomy: RAID 0/1/1+0/5 Serwer musi mieć możliwość rozbudowy o sprzętowy kontroler RAID zapewniający obsługę RAID 0,1,5,6 z 4GB pamięci cache z podtrzymywaniem bateryjnym.
Interfejsy sieciowe	Minimum 8 portów Ethernet 10/100/1000 Mb/s z funkcją Wake-On-LAN, RJ45, w tym 4 porty wbudowane, które nie zajmują slotów PCI-E.
Karta graficzna	Zintegrowana karta graficzna
Porty	3 x USB (w tym min. dwa USB 3.0). 1x VGA Wewnętrzny slot na kartę SD lub port USB. Możliwość rozbudowy o: - dodatkowy port VGA dostępny z przodu serwera,
Zasilacz	Minimum 2 szt., typ Hot-plug, redundantne o mocy 800W
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli), niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować

Element konfiguracji	Wymagania minimalne
	zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • dostęp do karty zarządzającej poprzez: - dedykowany port RJ45; - przez współdzielony port zintegrowanej karty sieciowej serwera • dostęp do karty możliwy: - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie.
Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych	Microsoft Windows Server min. w wersji 2012 Canonical Ubuntu Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware Citrix XenServer lub równoważne wsparcie systemów
Oprogramowanie do serwera	Licencja Microsoft Windows Server Standard 2016 wraz z 70 licencjami dostępowymi (per użytkownik) lub równoważna Zaoferowana licencja musi pozwalać na jej przenoszenie pomiędzy fizycznymi serwerami (np. w przypadku wymiany serwera) oraz ma zapewniać możliwość korzystania z wcześniejszych wersji oprogramowania.

5) Zakup przełączników 52 Port – 3 sztuki

Architektura sieci LAN	GigabitEthernet
SmartSwitch (WEB Managed)	Tak
Liczba portów 1000BaseT (RJ45)	48 szt.
Liczba portów COMBO GEth	2 szt.

(RJ45)/MiniGBIC (SFP)	
Liczba gniazd MiniGBIC (SFP)	4 szt.
Zarządzanie, monitorowanie i konfiguracja	• RMON - Remote Monitoring • zarządzanie przez przeglądarkę WWW
Obsługiwane protokoły i standardy	• IEEE 802.3 - 10BaseT • IEEE 802.3u - 100BaseFX • IEEE 802.3ab - 1000BaseT • IEEE 802.3z - 1000BaseSX/LX • IEEE 802.3x - Flow Control • IEEE 802.3az - Energy Efficient Ethernet • IEEE 802.2af • IEEE 802.1Q - Virtual LANs • IEEE 802.1p - Priority • SNMP - Simple Network Management Protocol • IEEE 802.1D - Spanning Tree • IEEE 802.1w - Rapid Convergence Spanning Tree • IEEE 802.1s - Multiple Spanning Tree • TACACS+ • QoS - Quality of Service (kontrola jakość usług i przepustowości) • DNS - Domain Name System • RMON - Remote Monitoring
Algorytm przełączania	Store-and-Forward
Prędkość magistrali wew.	104 Gb/s
Bufor pamięci	2 MB
Warstwa przełączania	3
Możliwość łączenia w stos	Tak

6) Zakup urządzenia wielofunkcyjnego - 2 sztuki

Funkcja	Opis
Ogólne	Pamięć: co najmniej 2 GB Dysk twardy: co najmniej 250 GB Pojemność wejściowa papieru: Co najmniej: 2 x 500-arkuszowe kasety na papier, obsługujące rozmiar papieru A5-A3 1 x 150-arkuszowa taca ręczna, obsługujące rozmiar papieru A6-SRA3 Pojemność wyjściowa papieru: co najmniej 250 arkuszy Drukowanie dwustronne, automatyczne (duplex) Uwierzytelnianie NFC
Funkcja druku	Druk laserowy; Prędkość drukowania: Czarno-białe: co najmniej 25 wydruków A4 na minutę Kolorowe: co najmniej 25 wydruków A4 na minutę Język opisu strony: PCL5e/c, PCL6, PostScript 3, XPS Rozdzielczość: co najmniej 1200 x1200 DPI

	Interfejs: 10-Base-T/100-Base-T/1,000-Base-T Ethernet, USB 3.0 Protokół sieciowy: TCP/IP (IP v4, IP v6), IPX/SPX, SMB, LPD, SNMP, HTTP, IPP/IPPS, AirPrint, Mopria Obsługiwane środowiska minimum: Windows® Vista/7/8/10, Windows®Server2008/2008R2/2012/2012R2, Sun®Solaris, RedHat® Linux, Macintosh OS , SAP® R/3® 3.x lub nowszy, mySAP ERP2004 lub nowszy lub równoważne
Funkcja kopiarki	Proces kopiowania: Elektrostatyczne kopiowanie laserowe. Prędkość kopiowania: Czarno-białe: co najmniej 25 kopii A4 na minutę Kolor: co najmniej 25 kopii A4 na minutę Rozdzielczość: co najmniej 600x600 dpi Zoom: przynajmniej 25 - 400%, krok co 0,1%
Funkcja skanera	Prędkość skanowania: co najmniej 80 obrazów na minutę przy 300 dpi Rozdzielczość: co najmniej 600 dpi Rozmiar oryginału: co najmniej od A6 do A3 Formaty wyjściowe: przynajmniej PDF/JPEG/TIFF/PDF z kompresją danych Sterowniki: Sieciowy przynajmniej TWAIN Skanowanie do: e-mail, SMB, FTP, WebDAV, Skanowanie do e-mail z linkiem do dokumentów. Zapisane adresy odbiorców: Pamięć na minimum 2000 adresów Książka adresowa: przez LDAP oraz lokalnie na dysku twardym
Podstawa	Oryginalna dedykowana przez producenta oferowanego urządzenia na kółkach umożliwiających jej przemieszczenie z szafką na np.: papier
Tonery	Urządzenia gotowe do pracy, wyposażone w pełnowartościowe zestawy tonerów oryginalnych sygnowanych logiem producenta oferowanego urządzenia.

7) Zakup firewall (UTM) – 1 sztuka

- Zapora sieciowa typu Next Generation Firewall (NGFW) lub równoważna
- Mechanizm pozwalający na dwustronną analizę ruchu.
- Minimalna ilość interfejsów:
  a) 7 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.
  b) 1 interfejs USB dla przyszłych potrzeb i do podłączenia modemu 3G
  c) 1 interfejs konsoli do zarządzania zaporą
- Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa
- Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji
- Możliwość utworzenia przynajmniej 50 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q
- Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej
- Minimalna ilość jednocześnie obsługiwanych połączeń: 90,000
- Możliwość obsłużenia przynajmniej 6000 nowych połączeń w ciągu 1 sekundy.
- Przepustowość urządzenia pracującego w trybie stateful firewall: 1,3 Gbps – dla ramki 1518B zgodnie z RFC 2544
- Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 900 Mbps

- Przepustowość urządzenia pracującego jako koncentrator VPN: 900 Mbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544
- Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 300 Mbps
- Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 20
- Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 25.
- Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.
- Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS (jak w punkcie 16) powinna wynosić minimum 100 Mbps oraz obsłużyć 250 połączeń.
- Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP
- Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site)
- Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa)
- Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP
- Wsparcie dla Dynamicznego DNS tzw. DDNS
- Zintegrowany mechanizm kontroli zawartości witryn zawierający minimum 20 Milionów URL w bazie pogrupowanych na kategorie tematyczne.
- Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate
- Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:
    a) wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron)
    b) wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony
    c) wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.
- Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps
- Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.
- Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.

- Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.
- Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN)
- Kontrola dostępności zestawionych tuneli VPN
- Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.
- Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.
- Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić)
- Funkcja NAT oparta o reguły bezpieczeństwa.
- NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)
- Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty.
- Skanowanie również plików skompresowanych.
- Zintegrowany system skanowania antyspyware
- Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.
- System IPS musi używać algorytmu szeregowego przetwarzania.
- Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
- Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji:
    a) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.
    b) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimporotwanie sygnatur
    c) Administrator systemu musi mieć możliwosc skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.
    d) System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
    e) Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa
    f) Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi
    g) Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p

h) Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń

Wymagane licencje:

1. Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji