GMINA BESKO
ul. Podkarpacka 5
Tel/fax 134673061 1346773520
ug@besko.pl
WWW.besko.pl
NIP 687-17-83-988
SR.271.16.2011

Besko, 2011-11-14

Zmiany w zapisach Specyfikacji Istotnych Warunków Zamówienia

Eliminacja wykluczenia cyfrowego w Gminie Besko

Str. 13 do 16
System zarządzania siecią WiMax

Jest:

Konsola zdalnej administracji
1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.

2. Zdalna instalacja wszystkich wersji programów na stacjach roboczych i serwerach Windows NT 4.0 sp6/ 2000/XP Professional/PC Tablet/2003/ Vista/Windows 7/ 2008.

3. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy

4. Komunikacja miedzy serwerem a klientami może być zabezpieczona hasłem.
5. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego
6. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.
7. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).
8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy.
9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
10. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
11. Możliwość tworzenia grup stacji roboczych/ serwerów i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
12. Możliwość importowania konfiguracji programu z wybranej stacji roboczej/serwera a następnie przesłanie (skopiowanie) jej na inną stację/ serwer lub grupę stacji roboczych w sieci.
13. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
14. Możliwość uruchomienia serwera zdalnej administracji na stacjach Windows NT4 (Service Pack 6)/2000/XP/Vista/Windows 7 oraz na serwerach Windows NT 4.0 (Service Pack 6)//2000/2003/2008 – 32 i 64-bitowe systemy.
15. Możliwość uruchomienia centralnej konsoli zarządzającej na stacji roboczej Windows 2000/XP/Vista/Windows 7, oraz na serwerach Windows 2000/2003/2008 - 32 i 64-bitowe systemy.
16. Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła.
17. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę w pełni kompatybilną z formatem bazy danych programu Microsoft Access.
18. Serwer centralnej administracji powinien oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle.
19. Do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache.
20. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) w formacie HTML lub CSV.
21. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta).
22. Serwer centralnej administracji powinien oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Synchronizacja ta, musi automatycznie

umieszczać komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie może wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny.

23. Serwer centralnej administracji powinien umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta, przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja musi otrzymać odpowiednią konfigurację.

24. Serwer centralnej administracji powinien być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania.

25. Serwer centralnej administracji powinien być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer powinien informować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośród puli nie zostało jeszcze wykorzystanych.

26. W sytuacji, gdy użytkownik wykorzysta wszystkie licencje, które posiada po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną powinien zostać poinformowany o tym fakcie za pomocą okna informacyjnego.

27. Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http.

28. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

29. Dostęp do kwarantanny klienta z poziomu systemu zdalnego zarządzania.

30. Możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu zdalnej administracji

31. Administrator powinien mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej

32. Podczas przywracania pliku, administrator powinien mieć możliwość zdefiniowania kryteriów dla plików które zostaną przywrócone w tym minimum: zakres czasu z dokładnością co do minuty kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta.

33. Możliwość utworzenia grup do których przynależność jest aplikowana dynamicznie na podstawie zmieniających się parametrów klientów w tym minimum w oparciu o: wersję bazy sygnatur wirusów, maskę wersji bazy sygnatur wirusów, nazwę zainstalowanej aplikacji, dokładną wersję zainstalowanej aplikacji, przynależność do domeny lub grupy roboczej, przynależność do serwera zdalnego zarządzania, przynależności lub jej braku do grup statycznych, nazwę komputera lub jej maskę, adres IP, zakres adresów IP, przypisaną politykę, czas ostatniego połączenia z systemem centralnej administracji, oczekiwania na restart, ostatnie zdarzenie związane z wirusem, ostatnie zdarzenie związane z usługą programu lub jego procesem, ostatnie zdarzenie związane ze skanowaniem na żądanie oraz z nieudanym leczeniem podczas takiego skanowania, maską wersji systemu operacyjnego oraz flagą klienta mobilnego.

34. Podczas tworzenia grup dynamicznych, parametry dla klientów można dowolnie łączyć oraz dokonywać wykluczeń pomiędzy nimi.
35. Utworzone grupy dynamiczne mogą współpracować z grupami statycznymi.

Powinno być:
Brak

Str. 21 do 22
Firewall
Jest:
Minimalne parametry zapory sieciowej typu Firewall znajdującej się na styku z siecią operatora zapewniającego dostęp do sieci Internet.
1. Urządzeniu musi realizować funkcję firewall i IPS (intrusion prevention system).
2. Przepustowość firewall'a na poziomie 300 Mbps.
3. Przepustowość łączna firewall i IPS: 150 Mbps.
4. Przepustowość dla ruchu szyfrowanego 3DES/AES: 170 Mbps.
5. Maksymalna liczba kanałów VPN: 250.
6. Maksymalna liczba sesji: 130 000.
7. Maksymalna liczba sesji na sekundę: 9 000.
8. Pamięć RAM min 1 GB.
9. Pamięć Flash min 64 MB.
10. Trzy zintegrowane interfejsy Ethernet 10/100 i dwa Ethernet 10/100/1000.
11. Jeden port konsoli, jeden port do transmisji szeregowej, dwa porty USB.
12. Obsługa protokołów RIP, OSPF, EIGRP, PIM.
13. Wbudowany serwer DHCP.
14. Obsługa IPv6.
15. Możliwość definiowania przydziału pasma i priorytetów dla wybranych klas ruchu.
16. Możliwość pracy w trybie transparentnym w warstwie 2
17. Funkcje translacji adresów NAT, PAT.
18. Analiza protokołów HTTP, FTP, ESMTP, DNS, SNMP, ICMP, SQL*Net, NFS, H.323, SIP, SCCP, MGCP, RTSP, TAPI i JTAPI, GPRS Tunneling Protocol (GTP), LDAP, ILS, RPC.
19. Sprawdzanie zgodności wykorzystywania analizowanych protokołów z procedurami RFC.
20. Dogłębna analiza sesji HTTP.
21. Kontrola ruchu typu pee-to-peer, instant messeging (IM) i aplikacji tunelowanych poprzez port 80, analiza Multipurpose Internet Mail Extensions (MIME).
22. Wykrywanie robaków i wirusów metodą korelacji zdarzeń w chronionej sieci z możliwością określania wagi dla danego ruchu, sygnatur, źródła ataku.
23. Funkcja IPS realizowana w dwóch trybach: in-line (ruch przechodzi przez IPS) i podsłuchu (ruch jest kopiowany do IPS) na bazie co najmniej 1400 sygnatur.
24. Obsługa do 100 sieci VLAN w standardzie 802.1Q.
25. Urządzenie musi mieć slot na jeden z poniższych modułów rozszerzeń:
a. moduł ochrony antywirusowej,
b. moduł IPS z pamięcią RAM 1 GB i flash 256 MB
c. moduł z czterema portami GigabitEthernet
26. Urządzenie musi umożliwiać konfigurację 2 wirtualnych urządzeń firewall, a po wykupieniu odpowiedniej licencji, do 5 wirtualnych firewall.

27. Firewall powinien zapewniać uwierzytelnianie w oparciu o Active Direktory, SecureID, Radius, LDAP.
28. Możliwość pracy redundantnej w trybie Active/Standby i Active/Active.
29. Zarządzanie za pomocą bezpiecznego połączenia HTTPS, SSH oraz lokalnie za pomocą kabla szeregowego.
30. Obsługa certyfikatów X.509 (SCEP, PKCS #7, #10, #12).
31. Dołączone oprogramowanie klienta VPN .
32. Certyfikaty ICSA Firewall, ICSA IPSec.
22
33. Obudowa umożliwiająca instalację w szafie rack 19", wysokość nie przekraczająca 1U.
Gwarancja: min. 2 lata gwarancji producenta

Powinno być:

Minimalne parametry zapory sieciowej typu Firewall znajdującej się na styku z siecią operatora zapewniającego dostęp do sieci Internet.

1. Urządzenie powinno pełnić rolę ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
2. Powinno być oparte o dedykowany system operacyjny – nie dopuszcza się rozwiązań gdzie platformą systemową jest otwarty system operacyjny np. UNIX (Linux, FreeBSD etc.) lub jego modyfikacja
3. Urządzenie nie powinno posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
4. Urządzenie musi posiadać co najmniej cztery porty 10/100 FastEthernet oraz jeden port 10/100 FastEthernet dla zarządzania OOB (Out of Band)
5. Powinno posiadać dedykowane dwa porty dla podłączenia konsoli oraz dla uzyskania zdalnego dostępu przez modem asynchroniczny
6. Powinno posiadać co najmniej jeden port USB dla przyszłych zastosowań (tokeny, etc.)
7. Powinno posiadać co najmniej 256MB DRAM oraz 64MB Flash
8. Urządzenie powinno posiadać dodatkowy slot pozwalający na wykorzystanie modułów funkcjonalnych zwiększających standardowe możliwości urządzenia, w szczególności:
    a. moduł umożliwiający osiągnięcie pełnej funkcjonalności systemu IPS (Intrusion Prevention System)
    b. moduł umożliwiający osiągnięcie funkcjonalności ochrony antywirusowej, antyspyware, antyspamowej, filtrowania i blokowania odwołań do niepożądanych adresów URL oraz filtrowania zawartości poczty elektronicznej e-mail
    c. uzyskanie co najmniej czterech dodatkowych portów 10/100/1000 GigabitEthernet
9. Oczekiwane jest, że w dostarczonym urządzeniu zaimplementowana będzie pełna funkcjonalność ochrony antywirusowej i antyspyware. Wymaga się, aby moduł obsługiwał dla tej funkcjonalności minimum 150 użytkowników – możliwość większej liczby po zastosowaniu dodatkowej licencji.
10. Urządzenie musi posiadać zintegrowane sprzętowe wsparcie dla szyfrowania
11. Urządzenie powinno mieć możliwość operowania jako transparentna ściana ogniowa warstwy drugiej ISO OSI
12. Urządzenie powinno umożliwiać terminowanie co najmniej 250 jednoczesnych sesji VPN opartych o protokół IPSEC
13. Na urządzeniu powinna istnieć możliwość terminowania jednocześnie 2 sesji WebVPN z możliwością rozbudowy do 250 sesji po zastosowaniu dodatkowej licencji.

14. Urządzenie powinno obsługiwać co najmniej 50 000 jednoczesnych sesji/połączeń z prędkością 9000 połączeń na sekundę
15. Przepustowość obsługiwana przez urządzenie nie powinna być mniejsza niż 300 Mbps i jednocześnie 170 Mbps dla ruchu szyfrowanego symetrycznymi algorytmami 3DES/AES
16. Wraz z urządzeniem powinno być dostarczane oprogramowanie klienta VPN, umożliwiające instalację go i zestawienie do urządzenia połączeń VPN z komputerów osobistych PC pracujących pod kontrolą systemów operacyjnych Windows, Solaris i Linux, a także komputerów Mac. Oprogramowanie to powinno pochodzić od tego samego producenta, co oferowane urządzenie i powinno być objęte jego jednolitym wsparciem technicznym.
17. Urządzenie powinno umożliwiać obsługę co najmniej 50 interfejsów VLAN w standardzie 802.1q.
18. Urządzenie powinno w celu redundancji umożliwiać implementację funkcji niezawodności pary takich urządzeń, czyli tzw. failover działającego w trybie active/standby lub active/active po zastosowaniu dodatkowej licencji.
19. Urządzenie powinno umożliwiać obsługę minimum 5 wirtualnych instancji firewall po zastosowaniu dodatkowej licencji.
20. Powinno dokonywać inspekcji ruchu voice w zakresie protokołów H.323, SIP, SCCP, MGCP, TAPI, JTAPI
21. Urządzenie powinno mieć możliwość blokowania aplikacji typu „internetowy komunikator" wykorzystujących port 80 (np.: Skype, MSN)
22. Urządzenie powinno mieć możliwość blokowania aplikacji typu peer-to-peer (np: Kaaza, eDonkoey)
23. Urządzenie powinno mieć możliwość inspekcji protokołów HTTP oraz FTP na nie standartowych portach
24. Urządzenie powinno zapewniać wsparcie dla list kontroli dostępu dla IPv6
25. Urządzenie powinno być zarządzalne przy wykorzystaniu dedykowanej aplikacji umożliwiającej płynną (z użyciem kreatorów) konfigurację poszczególnych funkcji urządzenia.
26. Urządzenie powinno być przystosowane do montażu w 19-in szafie rackowej i nie zajmować więcej miejsca niż 1RU (rack unit)

Gwarancja: min. 2 lata gwarancji producenta

Str. 30
Monitory
Jest:

Wymagane minimalne podstawowe parametry oraz warunki równoważności stawiane zamawianym monitorom:
a) Typ ekranu: Ekran ciekłokrystaliczny z matrycą wykonaną w technologii TFT-TN o przekątnej ekranu nie mniejszej niż 19",

b) Jasność: Nie mniejsza niż 250 cd/m2,

c) Kontrast statyczny: Nie mniejszy niż 1000:1,

d) Kąty widzenia (pion/poziom): 170/160 stopni,

e) Czas reakcji matrycy: max 5ms,

f) Złącza: złącza D-Sub oraz DVI-D,

g) Zakres pochylenia monitora: przynajmniej w zakresie od -5° do +15°,

h) Wbudowane przynajmniej 2 głośniki,

i) Możliwość zabezpieczenia - monitor musi być wyposażony w tzw. Kensington Slot,

j) Gwarancja: nie mniej niż 5 lat Wykonawcy projektu,

Powinno być:

Nazwa komponentu	**Wymagane minimalne parametry techniczne monitora**
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą TFT 19” (48,26cm) TN
Rozmiar plamki	0,284 mm
Jasność	250 cd/m2
Kontrast	1000:1 typowy (50 000:1 dynamiczny)
Kąty widzenia (pion/poziom)	160/160 stopni
Czas reakcji matrycy	max 5ms (czarny do białego)
Rozdzielczość maksymalna	1440 x 900 przy 60Hz
Częstotliwość odświeżania poziomego	30 – 83 kHz
Częstotliwość odświeżania pionowego	56 – 75 Hz
Wydłużenie w pionie	100 mm
Obrót monitora w pionie (PIVOT)	TAK
Obrót monitora w poziomie	+/-45 stopni
Pochylenie monitora	W zakresie od -4 do +21 stopni
Powłoka powierzchni ekranu	Antyodblaskowa
Podświetlenie	System podświetlenia 2 CCFL
Bezpieczeństwo	Monitor musi być wyposażony w tzw. Kensington Slot
Zużycie energii	Max. 50W przy max luminacji, włączonych głośnikach i aktywnych USB Typowe 18W Tryb uśpiony mniej niż 0,5W
Złącze	15-stykowe złącze D-Sub, złącze DVI-D, 4xUSB

Gwarancja	5 lat na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Gwarancja wymiany monitora w przypadku 1 uszkodzonego piksela
Certyfikaty	ISO 13406-2 lub ISO 9241, TCO 5.1, Energy Star 5.0, EPEAT GOLD
Inne	Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm Możliwość podłączenia do obudowy dedykowanych głośników lub głośniki wbudowane

Wójt Gminy Besko
Mariusz Bałaban