Szczegółowy opis przedmiotu zamówienia, załącznik numer 1A do SIWZ

1. Wymagania techniczne dla systemu bezpiecznego zdalnego dostepu do zasobów firmowych

Zamawiający oczekuje dostarczenia systemu bezpiecznego zdalnego dostępu do zasobów firmowych wraz z wdrożeniem, spełniającego następujące wymagania funkcjonalne i techniczne:

1. System musi być oparty o dedykowaną platformę sprzętową.
2. System musi być dostarczony i wdrożony w konfiguracji odpornej na awarię w trybie Active/Passive. Musi istnieć możliwość tworzenia konfiguracji nadmiarowej, w której węzły klastra zlokalizowane są w LAN bądź w odległych graficznie sieciach i komunikują się poprzez WAN.
3. Wsparcie dla różnych metod autentykacji/autoryzacji użytkowników:
    - Serwery RADIUS,
    - Usługi katalogowe LDAP, Microsoft Active Directory, Novel NDS/eDirectory,
    - Lokalna baza danych użytkowników,
    - System tokenowe, RSA SecureID,
    - Certyfikat X.509
4. System musi umożliwiać uwierzytelnianie dwuskładnikowe (hasło statyczne plus certyfikat, hasło dynamiczne plus certyfikat). Musi istnieć możliwość rozdzielenia serwera autentykacji użytkowników od serwera autoryzacji dostępu do zasobów.
5. System musi umożliwiać obsługę CRL poprzez http.
6. Możliwość tunelowania innych niż Web protokołów.
7. System musi oferować zróżnicowane metody dostępu do zasobów:
    - Dostęp podstawowy (m.in. aplikacje Web, standardowe protokoły pocztowe – IMAP, POP3, SMTP; współdzielenie plików - NETBIOS, NFS;usługi terminalowe – telnet, SSH),
    - Dostęp do aplikacji klient-serwer (enkapsulacja dowolnej aplikacji TCP w protokół https) bez konieczności zastosowania dodatkowych licencji,

- Pełen dostęp sieciowy bez konieczności zastosowania dodatkowej licencji – praca w trybie wysokiej dostępności (SSL). Możliwość automatycznego przełączania z trybu wysokiej wydajności do trybu wysokiej dostępności.

8. System musi umożliwiać dynamiczne przyznawanie praw dostępu do zasobów w zależności od spełnienia określonych warunków przez użytkownika zdalnego, węzeł zdalny, parametr sieci oraz parametry czasowe.
9. System musi umożliwiać szczegółową weryfikację stanu bezpieczeństwa węzła zdalnego. Musi istnieć możliwość:
    - Sprawdzenia obecności konkretnego procesu , pliku, wpisu w rejestrze Windows,
    - Sprawdzenie czy włączono odpowiednie usługi zabezpieczeń zarówno w momencie logowania jak i w trakcie trwania sesji,
    - Sprawdzenie czy wszystkie pobierane pliki pośrednie i pliki tymczasowe instalowane w czasie logowania są usuwane w momencie wylogowania,
    - Sprawdzenie przed zalogowaniem takich atrybutów jak adres IP, typ przeglądarki, certyfikaty cyfrowe.
    - Integracja z systemami weryfikacji stanu bezpieczeństwa firm trzecich
10. System musi zapewniać możliwość współpracy z rozwiązaniem klasy NAC tego samego producenta w zakresie jednokrotnego uwierzytelnienia użytkowników, tj. status uwierzytelnienia użytkownika na urządzeniu dostępowym SSL jest automatycznie i w sposób przezroczysty dla użytkownika przekazywany do urządzenia kontrolującego infrastrukturę NAC.
11. System musi być zarządzany przez przeglądarkę Web.
12. System musi umożliwiać spójne zarządzanie z jednej konsoli administracyjnej wieloma urządzeniami w przypadku buforowania konfiguracji nadmiarowych.
13. System musi umożliwiać wykonywanie lokalnych kopi zapasowych konfiguracji lub na zewnętrznym serwerze FTP oraz SCP.
14. System musi umożliwiać integrację z zewnętrznymi serwerami SNMP v2 oraz SYSLOG.
15. System oprócz wersji aktywnej oprogramowania, musi przechowywać minimum dwie wersje poprzednie oraz umożliwiać reset do wersji fabrycznej.

16. System musi zapewniać możliwość zorganizowania indywidualnych bezpiecznych sesji online między użytkownikami za pomocą interfejsu webowego wraz z możliwością przejęcia kontroli nad konsolą i aplikacją drugiego użytkownika. Licencja musi zapewniać możliwość obsługi co najmniej 200 użytkowników oraz 100 sesji.
17. System musi mieć możliwość rozbudowy do obsługi minimum 1000 jednoczesnych klientów SSL VPN.
18. System powinien zostać dostarczony z licencjami umożliwiającymi pracę w konfiguracji odpornej na awarię w trybie Active/Passive oraz zapewniać obsługę minimum 100 jednoczesnych klientów SSL VPN.
19. System powinien być dostarczony z serwisem producenta na okres 36 miesięcy na poziomie Następny Dzień Roboczy, co oznacza czas wysyłki urządzenia zastępczego w przypadku awarii/uszkodzenia sprzętu.

2. Odnowienie licencji VMWARE VCenter

Zamawiający ponadto oczekuje dostarczenia supportu, przedłużenia subskrycpji i wsparcia producenta na poziomie podstawowym (Basic Support and Subcription) dla produktu VMware vCenter Server 4 Standard for vSphere (Includes Orchestrator and Linked Mode) na okres do 31.12.2013r. VMware Customer number 5619282484. Obecny suport wygasł 16.11.2010r.