

Opis przedmiotu zamówienia

Dla zadania pn. „Zakup urządzenia Fortianalyzer VM”

1. Przedmiot zamówienia:

Zamówienie dotyczy zakupu i dostawy analizatora i kolektora ruchu sieciowego FortiAnalyzer VM dla posiadanego przez Zamawiającego urządzenia UTM Fortigate 800C.

2. Minimalne wymagania techniczne i funkcjonalno-użytkowe:

Dostarczony system musi spełniać następujące wymagania:

- 1) musi być dostarczony w postaci wirtualnej, jako virtual appliance. Obsługa platform wirtualizacyjnych: VMware vSphere, Xen, KVM, Hyper-V;
- 2) musi być stale rozwijany i posiadać aktualną dokumentację techniczną;
- 3) musi posiadać wsparcie techniczne na okres co najmniej 1 roku;
- 4) musi umożliwiać:
 - a) zbieranie w czasie rzeczywistym logów z urządzenia UTM Fortigate firmy Fortinet;
 - b) tworzenie raportów na podstawie wybranych przez użytkownika kryteriów;
 - c) wizualizację danych w postaci graficznej;
 - d) tworzenie oraz modyfikację szablonów PDF służących do generowania raportów oraz ich import/eksport;
 - e) powiadamianie użytkownika o zdarzeniach systemowych za pomocą wiadomości e-mail pakietów SNMP oraz wiadomości syslog;
 - f) archiwizację zbieranych danych;
 - g) wyświetlanie zebranych logów w czasie rzeczywistym oraz prezentację danych archiwalnych;
 - h) przeglądanie logów z podziałem na wirtualne domeny skonfigurowane na urządzeniu;
 - i) filtrowanie logów oraz ich przeszukiwanie według podanych przez użytkownika kryteriów;
 - j) identyfikację aplikacji na poziomie 7 warstwy OSI przy wyświetlaniu zebranych danych oraz wizualizację ich użycia w sieci;
 - k) wyświetlanie informacji o użyciu łącz VPN, w tym IPSec VPN oraz SSLVPN;
 - l) wyświetlanie informacji o aktywności użytkowników w sieci na podstawie używanych przez nich kont domenowych;
 - m) wyświetlanie informacji o zablokowanych infekcjach wirusowych;
 - n) wyświetlanie informacji o zablokowanych atakach sieciowych przez moduł IPS;
 - o) dostęp do API zgodnego ze standardami JSON oraz XML;
 - p) zbieranie logów w trybie kolektora lub analizatora (do wyboru);
 - q) szyfrowaną transmisję logów z urządzenia Fortigate do kolektora;
 - r) system powinien obsługiwać co najmniej 2 interfejsy vNIC Ethernet 10/100/1000 oraz obsługiwać powierzchnię dyskową min. 96 TB.

3. Licencja

Licencja bezterminowa na korzystanie z rozwiązania FortiAnalyzer VM. Licencja powinna pozwalać na gromadzenie min. 6 GB logów/dzień oraz min. 3,5 TB pojemności. Nielimitowane GB/Dzień w przypadku używania w trybie kolektora.

4. Gwarancja

Gwarancja w formie wsparcia technicznego na okres 12-stu miesięcy. W ramach wsparcia technicznego system powinien posiadać subskrypcję umożliwiającą dostęp do najnowszych wersji oprogramowania (firmware). Zgłoszenia serwisowe będą przyjmowane w trybie 8x5/24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5/24x7.