Opis Przedmiotu Zamówienia

Zakup wsparcia technicznego dla węzła bezpieczeństwa MAN Wrocław [2022]

1. Specyfikacja techniczna

Przedmiot zamówienia

Przedmiotem zamówienia jest rozbudowa posiadanej przez zamawiającego platformy bezpieczeństwa CheckPoint o zestaw 2 urządzeń rozszywających ruch SSL wraz z wymaganymi licencjami i dedykowaną platformą zarządzającą.

Głównym celem rozwiązania jest podniesienie poziomu bezpieczeństwa aplikacji, pracujących w oparciu o protokół SSL/TLS, poprzez możliwość poddania ich inspekcji przez systemy bezpieczeństwa posiadane przez Zamawiającego.

Rozwiązanie ma za zadanie deszyfrację całego ruchu przychodzącego do urządzenia, następnie ruch rozszyfrowany przesyłany jest do rozwiązań bezpieczeństwa, które dokonują jego analizy pod kontem pojawiających się zagrożeń lub naruszeń polityki bezpieczeństwa, a następnie przeskanowany ruch wraca ponownie do urządzenia, gdzie może zostać ponownie zaszyfrowany.

Podstawowe funkcjonalności rozwiązania

Oferowane rozwiązanie ma posiadać możliwość uruchomienia m.in. następujących modułów funkcjonalnych:

- SSL Inspect,
- SSLI Dashboard,
- Operator Tool Box,
- Advanced Routing,
- URL Filtering,

Podstawowe funkcjonalności modułu SSL Inspection

Główne cechy SSL Inspection:

- Możliwość precyzyjnego zarządzania szyfrowanym ruchem aplikacyjnym.
- Brak degradacji wydajności (operacje kryptograficzne akcelerowane sprzętowo).
- Uproszczone zarządzanie materiałem kryptograficznym (centralizacja na urządzeniu).
- Skalowalność rozwiązania.
- Minimalizacja opóźnień z uwagi na szeregowe operacje szyfrowania i deszyfracji.
- Optymalizacja wykorzystania systemów bezpieczeństwa.

2. Specyfikacja urządzeń

Urządzenia mają mieć możliwość instalacji w formie klastra wysokiej dostępności (HA) pracującego w trybie Active/Passive lub Active/Active (zgodnie z zaplanowaną architekturą docelową). Poniżej zestawione są cechy fizyczne urządzenia:

- Karta akcelerująca operacje kryptograficzne – Intel QuickAssist (nowa technologia kart oferująca podniesioną wydajność dla transakcji SSL/TLS opartych o krzywe eliptyczne, co obecnie uważa się za najbezpieczniejszy algorytm)
- Liczba wirtualnych instancji vADC – 2 z możliwością rozbudowy do 22 vADC
- Liczba połączeń SSL na sekundę, 2K RSA – 20 500
- Liczba połączeń SSL na sekundę, EC-P256 – 10 000
- Przepustowość ruchu SSL – 9 Gbps
- Przepustowość całkowita urządzenia – 20 Gbps
- Pamięć RAM – 32 GB
- Liczba interfejsów – 2x10GbE SFP+ SR (wkładki światłowodowe), 8x1GbE 1000BASE-T
- Dysk 500GB SSD,
- Dwa redundantne zasilacze AC
- Wysokość urządzenia 1U

Oferowana platforma ma pozwalać na utworzenie wirtualnych instancji ADC będących od siebie w pełni odseparowanych, uruchomionych w ramach tego samego urządzenia. W konsekwencji jedno urządzenie fizyczne ma możliwość pracy jako kilka niezależnych platform. Główne cechy urządzenia:

- Separacja vADC dla aplikacji, departamentu lub grupy funkcyjnej.
- vADC między sobą nie konkurują o zasoby – każdy z nich ma przydzieloną, odseparowaną pulę zasobów możliwą do modyfikacji w dowolnym momencie).
- Kompletna izolacja na wypadek błędów.
- Skalowalność vADC nie mająca wpływu na pozostałe wirtualne instancje.
- Łatwa i szybka migracja vADC w momencie, gdy większa wydajność jest konieczna.

Każda z wirtualnych instancji posiada pełną separację zarządzania, kontroli błędów, interfejsów i konfiguracji (routing, VLAN) sieciowych (mogą być

również współdzielony pomiędzy kilka vADC), komponentów sprzętowych (pamięć RAM, CPU, zasoby dyskowe). Izolacja vADC posiada certyfikację ***Electronic Warfare Associates, Inc.*** w zakresie pełnej izolacji i rezerwacji zasobów vADC gwarantującą wymagany poziom SLA dla aplikacji.

Przydzielanie zasobów wirtualnym instancjom vADC odbywa się z wykorzystaniem Capacity Units, które stanowią unikatowy kwantyfikator przydzielania zestawu zasobów, takich jak:

- Moc obliczeniowa procesorów sieciowych (SP)
- Pamięć RAM
- Przestrzeń dyskowa

Wartość przydzielonych Capacity Units może być edytowalna w dowolnym czasie w cyklu życia rozwiązania. Precyzyjny przydział Capacity Units gwarantuje separację i rezerwację zasobów dla każdej z wirtualnych instancji. Rozwiązanie zapewnia brak wpływu problemów wydajnościowych jednej instancji vADC na inne, tak by:

- Zagwarantować wszystkim wirtualnym instancjom odpowiedni poziom wydajności konieczny do szybkiego i efektywnego realizowania polityki bezpieczeństwa aplikacji.
- Osiągnąć brak inwazyjności dla pozostałych instancji vADC.

Każda z wirtualnych instancji vADC powinna posiadać możliwość pracy na różnej (dowolnej) wersji systemu operacyjnego urządzenia.

3. Specyfikacja Systemu zarządzania

Systemem centralnego zarządzania pozwalający na zarządzanie, monitorowanie oraz administrowanie wieloma urządzaniami z jednego punktu. Platforma zarządzająca dostarczona jest w formie oprogramowania.

Podstawowe funkcjonalności systemu w zakresie zarządzania:

- Wbudowany system zbierania i korelacji logów służący do raportowania zdarzeń historycznych i analizy ataków. System pozwala na tworzenie skorelowanych raportów, analizę trendów, konfigurowalne pulpity nawigacyjne, kontrolę dostępu opartą na rolach/użytkownikach, zaawansowane alerty, raporty śledcze i raporty zgodności.
- System zawiera ujednolicone narzędzie raportowania dla wszystkich modułów zabezpieczeń sprzętowych. Dane z wielu urządzeń są zbierane, oceniane i udostępniane w skonsolidowanym widoku pulpitów nawigacyjnych i raportów.
- Dostęp można kontrolować dzięki obsłudze kontroli dostępu opartej na rolach (RBAC) w systemie.
- System obsługuje raporty i alerty, które można dostosować dla każdego

użytkownika (lub klienta), umożliwiając zarządzanie i kontrolę wielu dzierżawców.

- System umożliwia przesyłanie wiadomości do zewnętrznego serwera logów. Filtr przesyłanych logów ma możliwość skonfigurowania pod kątem obiektu oraz ważności. Wszystkie zdarzenia generowane przez urządzenie mogą być przesyłane za pomocą protokołu syslog.
- System umożliwia przesłanie informacji o zdarzeniach i alarmach za pomocą protokołów syslog i SNMP. System umożliwia wysłanie takiej informacji do wielu systemów docelowych
- Możliwość zdefiniowania automatycznego harmonogramu raportowania, który może być dystrybuowany automatycznie, bez udziału administratora.
- Możliwość filtrowania i sortowania wewnątrz raportów.
- Możliwość tworzenia raportów w formacie HTML, CSV oraz XLS.
- Możliwość uwierzytelniania użytkowników za pośrednictwem serwerów RADIUS.
- Wsparcie dla protokołu SNMP v3.
- Dostęp do systemu z poziomu przeglądarki www bez konieczności instalowania dodatkowego klienta.
- Wsparcie dla protokołu SSH.
- Obsługa REST API dla integracji z systemami firm trzecich. Interfejs REST API umożliwia konfigurację wszystkich elementów systemu.
- Zarządzanie „out-of-band”.
- Możliwość jednoczesnej pracy wielu administratorów, którzy mogą być zalogowani w tym samym czasie przez GUI.
- Audyt wszelkich zmian administracyjnych dokonanych na urządzeniu.
    - Możliwość wysyłania alarmów po przekroczeniu określonych progów (ruch, miejsce na dysku, użycie pamięci, użycie procesora itd.).
    - Powiadomienia o zdarzeniach poprzez e-mail.
    - Obsługa i przechowywanie dwóch instancji systemu operacyjnego oraz możliwość aktywacji i dezaktywacji każdej z nich w razie potrzeby.

4. Kontrakty Serwisowe

Kontrakty serwisowe muszą zapewniać:

- Dostęp do aktualizacji oprogramowania i możliwość aktualizacji oprogramowania oraz możliwości zmiany wersji oprogramowania na

nowszą, gdy taka zostanie wydana przez producenta oprogramowania;
- Naprawę wszystkich Wad Sprzętu lub wymianę Sprzętu, w przypadku, gdy naprawa nie jest możliwa. Naprawy będą wykonywane w siedzibie Zamawiającego;
- Aktualizację kategoryzacji treści internetowych (URL Filtering) w ramach dostarczonej subskrypcji.

5. Warsztaty

1) Wykonawca przeprowadzi 2 dniowe warsztaty dla wskazanych przez Zamawiającego Administratorów (nie więcej niż 3 osoby) w zakresie instalacji, konfiguracji, diagnostyki i zarządzania serwisowanym systemem.
2) Warsztaty powinny obejmować poniższe zagadnienia:
   - Wprowadzenie do technologii
     - Omówienie najważniejszych funkcji i licencjonowania
   - Podstawowa konfiguracja
     - Konfiguracja zarządzania systemem
     - Zarządzanie konfiguracjami i wersjami systemu
   - Konfiguracja elementów sieciowych
     - Konfiguracja VLAN, STP
     - Konfiguracja portów fizycznych
     - Konfiguracja interfejsów IP oraz routingu
   - Konfiguracja SLB
   - Akceleracja SSL
     - Ogólna koncepcja SSL Offloading
     - Budowanie polityki deszyfracji SSL
     - Zarządzanie polityką oraz certyfikatami
   - Content Load Balancing
     - Koncepcja Content Switching
     - Definiowanie reguł dla HTTP
   - Wysoka dostępność
     - Omówienie HA
     - Konfiguracja
   - Troubleshooting

6. Wymagania ogólne

1) Wykonawca zobowiązuje się do świadczenia w ramach Usługi Wsparcia Technicznego przez konsultantów Wykonawcy bieżących konsultacji telefonicznych w zakresie eksploatacji Urządzeń, w szczególności przez wyjaśnienia, diagnozy, porady i odpowiedzi na pytania związane z eksploatacją Urządzeń. Jak również pomocy w przypadku trudności z wykonaniem prac administracyjnych i konfiguracyjnych.
2) Wsparcie producenta dla Urządzeń musi być potwierdzone przez polskie lub regionalne przedstawicielstwo/oddział producenta

Sprzętu/Oprogramowania.

3) W ramach dostarczonych kontraktów serwisowych i świadczonej na rzecz Zamawiającego Usługi Wsparcia Technicznego Wykonawca będzie usuwał wszystkie Wady Urządzeń.
4) Wykonawca zobowiązuje się do dostarczania urządzeń oraz podzespołów wynikających z realizacji umowy na swój koszt i ryzyko, własnym transportem po uprzednim uzgodnieniu terminów dostawy z Zamawiającym.
5) Urządzenia oraz podzespoły dostarczone zostaną wraz ze wszystkimi akcesoriami niezbędnymi do umożliwienia ich montażu w określonej lokalizacji na terenie miasta Wrocławia.
6) W przypadku braku możliwości naprawy uszkodzonego sprzętu Zamawiający dopuszcza wymianę sprzętu na taki sam Sprzęt jak Sprzęt uszkodzony. Dostarczony zamienny sprzęt musi być nowy, musi być dostarczony z legalnego kanału dystrybucji producenta sprzętu, musi być objęty gwarancją i wsparciem na zasadach określonych w niniejszej Umowie. Wymiana nastąpi niezwłocznie po uzyskaniu przez Wykonawcę informacji o braku możliwości naprawy uszkodzonego Sprzętu.
7) Wady Urządzeń będą zgłaszane przez Zamawiającego za pomocą poczty elektronicznej przekazanej na wskazane adresy lub numery telefonów kontaktowych Wykonawcy określone w pkt 10).
8) Wykonawca będzie przyjmował Zgłoszenia serwisowe (przez które należy rozumieć zgłoszenie Wady Urządzeń) w trybie ciągłym, tzn. przez 24 godziny w ciągu doby, przez 7 dni w tygodniu, przez wszystkie dni w roku.
9) Nie później niż 7 dni po zgłoszeniu usunięcia awarii Wykonawca przedstawi Zamawiającemu protokół reakcji na awarię, celem jego uzgodnienia z Zamawiającym w terminie 5 Dni Roboczych, w którym zawrze on następujące informacje:

    a) termin zgłoszenia niedostępności usługi lub zgłoszenia innej awarii,
    b) czas zgłoszenia reakcji na awarię,
    c) czas zgłoszenia usunięcia awarii,
    d) nazwę niedostępnej usługi, opis awarii oraz miejsce gdzie wystąpiła awaria,
    e) dodatkowe informacje związane z wystąpieniem awarii oraz mające wpływ na jej usunięcie,
    f) określenie wysokości kary umownej, jeżeli w danym przypadku takie naliczenie przysługuje Zamawiającemu.

10) Wykonawca - poza przypadkami, gdy samodzielnie wykryje Wadę o nienależytym wykonywaniu umowy lub niewykonaniu umowy, a także o wszelkich wadach Sprzętu, zostanie poinformowany przez Zamawiającego

drogą:

a) telefoniczną – na numer telefonu Wykonawcy: ....., lub
b) elektroniczną – na adres e-mail Wykonawcy: .....

11) Informacja o nienależytym wykonywaniu umowy lub niewykonaniu umowy, a także o wszelkich Wadach Sprzętu lub kontraktów serwisowych zostanie uznana za dostarczoną w przypadku przekazania jej za pomocą jednego z kanałów komunikacyjnych, o których mowa w pkt 10). Przekazanie informacji jednym ze sposobów, o których mowa w pkt 10), nie wyklucza zastosowania innych sposobów wymienionych w tym ustępie lub innych sposobów w nim nie wskazanych (np. doręczenie za pomocą poczty czy doręczenie osobiste).