UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

Załącznik nr 3 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa dwóch identycznych urządzeń klasy firewall wraz z usługą wdrożenia wykorzystywanej obecnie konfiguracji środowiska produkcyjnego zgodnie z podanym poniżej opisem technicznym.

Zamawiający wymaga uruchomienia dostarczonego sprzętu we wskazanym miejscu z zachowaniem ciągłości działania usług opartych na ww. urządzeniach. Zamawiający wymaga zapewnienia gwarancji producenta na urządzenia w okresie 60 miesięcy od daty podpisania protokołu odbioru i opieki technicznej autoryzowanego serwisu partnera producenta przez cały okres trwania gwarancji. Opieka techniczna powinna zawierać m.in.:

- ❖ wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu,
- ❖ wymianę uszkodzonego sprzętu (producent wysyła sprzęt następnego dnia roboczego),
- ❖ dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

Dostarczone urządzenia muszą:

- ❖ zachować posiadane przez zamawiającego funkcjonalności (Firewall, NAT, IPSec, Routing, URL Filtering, AppSecure).
- ❖ być dostarczone z licencjami na okres 60 miesięcy, jeżeli są niezbędne do utrzymania, uruchomienia funkcjonalności.
- ❖ być dostarczone wraz z niezbędnym okablowaniem umożliwiającym podpięcie i uruchomienie sprzętu w lokalizacjach Uniwersytetu: (odpowiednie okablowanie zasilające, wkładki SPF+ minimum 32 sztuki (SM do 10 km), patchcordy światłowodowe LC-LC minimum 26 sztuk (1,5 m - 2 m)

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

OPIST TECHNICZNY (dwóch urządzeń o tej samej konfiguracji)

1. Firewall musi być dostarczony jako dedykowane urządzenie sieciowe w postaci chassis o wysokości 1U, przystosowane do montażu w szafie rack, wyposażone w dwa wymienne zasilacze AC. Warunkiem koniecznym jest możliwość wymiany zasilaczy w trakcie pracy urządzenia.
2. System operacyjny firewalla ma być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny powinien odpowiadać za sterowanie i monitorowanie pracy komponentów firewalla. Ruch tranzytowy użytkowników przechodzący przez firewall nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Konieczna jest dostępność opcji uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym. Moduł kontrolny musi posiadać dedykowany interfejs Ethernet przeznaczony do zarządzania out-of-band.
3. Zarządzanie firewallem powinno odbywać się przy pomocy tekstowego interfejsu użytkownika (dostępnego przez port konsoli, telnet, ssh) oraz przy pomocy graficznego interfejsu użytkownika WWW. Wymagana jest możliwość zarządzania przez centralny system zarządzający tego samego producenta (należy go dostarczyć w postaci hardware appliance lub wirtualnej maszyny zgodnej z MS Hyper-V 2019) lub posiadany przez Zamawiającego Junos Space Security Director
4. System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. Obsługa ruchu tranzytowego użytkowników musi być realizowana sprzętowo. System operacyjny firewalla musi śledzić stan sesji użytkowników (*stateful processing*), tworzyć i zarządzać tablicą stanu sesji.
5. Firewall winien być wyposażony w:
   - w nie mniej niż 8 interfejsów 10 Gigabit Ethernet SFP+
   - w min. 2 interfejsy 10 Gigabit Ethernet SFP+ dedykowane do zestawienia klastra niezawodnościowego z drugim firewallem.
   - nie mniej niż 64 GB pamięci RAM oraz dysk M.2 SSD o pojemności min. 240 GB z 1+1 RAID.
6. Z punktu widzenia systemu operacyjnego firewalla wszystkie usługi bezpieczeństwa powinny być zdefiniowane w tym samym pliku konfiguracyjnym zdefiniowanym na module kontrolnym.

7. Firewall musi umożliwiać:
    - wykorzystywanie polityki ACL bez kontroli stanu sesji (stateless ACL) oraz na wykorzystywanie polityki Stateful Firewall.
    - realizowanie zadania Stateful Firewall z wydajnością nie mniejszą niż 44 Gb/s liczoną dla ruchu IMIX. Firewall musi obsłużyć nie mniej niż 10 milionów równoległych sesji oraz być w stanie zestawić nie mniej niż 500 tysięcy nowych połączeń/sekundę.
    - obsługę funkcji Application Firewall bez potrzeby wykupywania dodatkowej licencji. Przepustowość inspekcji Application Firewall powinna być nie mniejsza niż 40 Gb/s.
    - zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site.
    - obsługę ruchu szyfrowanego o przepustowości nie mniejszej niż 30 Gb/s dla ruchu IMIX.
    - zezwalanie na zestawianie tuneli GRE oraz IP-IP.
    - na ochronę przed atakami DoS oraz DDoS.
8. Polityka bezpieczeństwa systemu zabezpieczeń powinna uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 60 000 reguł polityki bezpieczeństwa.
9. Firewall musi posiadać możliwość rozbudowy poprzez:
    - zastosowanie licencji, o funkcję wykrywania i blokowania ataków intruzów (IPS) realizowaną z wydajnością co najmniej 27 Gbps. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall.
    - zastosowanie licencji, o funkcje inspekcji antywirusowej, inspekcji antyspamowej oraz filtrowania dostępu na podstawie adresów URL.
    - zastosowanie licencji, o mechanizm ochrony przed atakami 0-day na podstawie inspekcji sandbox realizowanej w chmurze obliczeniowej producenta.
    - mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz przycinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków IP, TCP i UDP.
    - tworzenie osobnych kolejek dla różnych klas ruchu, a kolejki muszą posiadać wsparcie dla mechanizmu WRED

10. Urządzenie powinno obsługiwać:
    - protokoły dynamicznego routingu: RIP, OSPF, IS-IS oraz BGP.
    - minimum 2 miliony prefiksów w tablicy RIB oraz 1.2 miliona w tablicy FIB.
    - protokoły odpowiedzialne za przesyłanie ruchu multicastowego, w tym IGMPv2, PIM-SM, PIM-DM, PIM-SSM, SDP, DVMRP oraz MSDP.
11. Urządzenie musi wspierać protokół MPLS i pozwalać na zestawianie połączeń MPLS L3VPN.
12. Firewall powinien posiadać możliwość pracy w konfiguracji odpornej na awarie opartej o klastrowanie urządzeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
13. Administratorzy winni mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.
14. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce i być świadczone w języku polskim.
15. Całość dostarczanego sprzętu i oprogramowania powinna pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.

SZKOLENIA

Wymagane jest zapewnienie szkolenia z zakresu konfiguracji i zarządzania dostarczonymi urządzeniami. Szkolenie powinno być przeprowadzone dla 3 osób w języku polskim i trwać m.in. 10 dni roboczych.
Zakres szkolenia musi zawierać obszary dotyczące:

- Systemu operacyjnego dostarczonego urządzenia
- Przygotowania urządzeń do pracy
- Obsługi CLI dostarczonego urządzenia
- Konfigurację podstawowych ustawień sieciowych m.in. (konta użytkowników, Logi, NTP, pliki konfiguracyjne, SNMP
- Monitorowania pracy i utrzymania systemu m.in. monitorowania urządzeń, narzędzi sieciowych, aktualizację systemu, odzyskiwanie haseł)
- Konfiguracji interfejsów
- Routingu (routing statyczny, OSPF, Protokół BGP)
- Polityki routingu i filtrowanie pakietów
- Class of Service
- Load Balancing i Filter Based Forwarding
- Niezawodności i funkcji HA
- Security (zagadnienia polityk bezpieczeństwa, identyfikacja i implementacja aplikacji, wykrywanie oraz blokowanie intruzów, (IPS), koncepcja i konfiguracja ruchu szyfrowanego, Analiza Zagrożeń, Analiza Logów)
- Przełączania w sieciach warstwy drugiej na urządzeniach od producenta Firewall
- Wirtualizacji sieci (Konfiguracja i monitorowanie sieci VLAN, Voice VLAN, Native VLAN, Interfejsy VLAN w warstwie trzeciej
- Spinning Tree, BPDU Protection, Loop Protection, Root Protection, Limitowanie adresów Mac na portach, DHCP Snooping, IP Source Guard, Dynamic ARP Inspection, MSTP, VSTP
- Bezpieczeństwa i filtrowanie ruchu
- Ochrony i Bezpieczeństwa w warstwie L2
- Zaawansowanego przełączania (MVRP, L2PT)
- Uwierzytelniania i kontroli dostępu (8 02.1X, MAC RADIUS
- Telefonii IP (Konfiguracja Power over Ethernet, LLDP, LLDP-MED