Załącznik nr 4 do SWZ

Opis przedmiotu zamówienia pn. Dostawa klastra firewalli dla CI TASK.

1. Firewall musi być dostarczony jako dedykowane urządzenie sieciowe o wysokości maksymalnie 3U, przystosowane do montażu w szafie rack, wyposażone w co najmniej dwa redundantne zasilacze AC. Musi istnieć możliwość wymiany zasilaczy w trakcie pracy urządzenia.
2. Maksymalny sumaryczny pobór mocy urządzenia nie może przekroczyć 1000W.
3. System operacyjny firewalla musi być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny musi 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. Musi być dostępna opcja 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.
4. Zarządzanie firewallem musi odbywać się przy pomocy tekstowego interfejsu użytkownika (dostępnego przez port konsoli, telnet, ssh) oraz przy pomocy graficznego interfejsu użytkownika WWW.
5. Urządzenie musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Uwierzytelnianie administratorów musi się odbywać za pomocą lokalnej bazy urządzenia oraz serwera RADIUS lub TACACS+.
6. Musi istnieć możliwość podziału urządzenia na mniejsze części logiczne (nazywane wirtualnymi systemami/firewallami). System musi obsługiwać co najmniej 32 takie systemy.
7. Każdy wirtualny system/firewall musi mieć możliwość konfiguracji niezależnych i odrębnych polityk bezpieczeństwa oraz niezależnego zatwierdzania konfiguracji które w jakikolwiek sposób nie mogą być widoczne w pozostałych systemach wirtualnych.
8. 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 rutingu IP, odpowiedzialny za ustalenie tras rutingu 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.
9. Firewall musi być wyposażony w nie mniej niż 8 portów SFP+ 10 Gigabit Ethernet obsługujących również moduły SFP Gigabit Ethernet. Wszystkie porty muszą być wyposażone w kompatybilne moduły SFP+ SM 1310nm DDM.
10. Firewall musi być dodatkowo wyposażony w nie mniej niż dwa porty (SFP+ 10 Gigabit Ethernet lub QSFP+ 40 Gigabit Ethernet) dedykowane do zestawienia klastra HA z drugim firewallem. Porty te muszą być wyposażone w kompatybilne moduły SFP+ lub QSFP+ SM 1310nm DDM.
11. Urządzenie musi być wyposażone w nie mniej niż 64 GB pamięci RAM oraz w dwa dyski SSD o pojemności co najmniej 240 GB każdy pracujące w systemie RAID 1.
12. Z punktu widzenia systemu operacyjnego firewalla wszystkie usługi bezpieczeństwa muszą być zdefiniowane w tym samym pliku konfiguracyjnym zdefiniowanym na module kontrolnym.
13. Firewall musi umożliwiać wykorzystanie polityk ACL bez kontroli stanu sesji (stateless ACL) oraz na wykorzystanie polityk Stateful Firewall.

14. Firewall musi realizować zadania Stateful Firewall z wydajnością nie mniejszą niż 20 Gb/s liczoną dla ruchu IMIX. Firewall musi obsłużyć nie mniej niż 5 milionów równoległych sesji oraz być w stanie zestawić nie mniej niż 170 tysięcy nowych połączeń/sekundę.
15. Firewall musi obsługiwać translację adresów IP (NAT) statyczną oraz dynamiczną dla protokołów IPv4 oraz IPv6.
16. Firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania. Identyfikacja aplikacji musi się odbywać co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów. Przepustowość przy aktywnej inspekcji powinna być nie mniejsza niż 18 Gb/s.
17. Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. Firewall musi obsługiwać ruch szyfrowany o przepustowości nie mniejszej niż 5Gb/s dla ruchu IMIX. Firewall musi pozwalać na zestawienie co najmniej 7000 tuneli typu site-to-site oraz 7000 tuneli client-to-site.
18. Firewall musi pozwalać na zestawianie tuneli GRE oraz IP-IP.
19. Firewall musi posiadać mechanizmy pozwalające na ochronę przed atakami DoS oraz DDoS.
20. Polityka bezpieczeństwa systemu zabezpieczeń musi 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 50 000 reguł polityki bezpieczeństwa.
21. Firewall musi posiadać możliwość rozbudowy, poprzez zastosowanie licencji, o funkcję wykrywania i blokowania ataków intruzów (IPS) realizowaną z wydajnością co najmniej 10 Gbps. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall.
22. Firewall musi posiadać możliwość rozbudowy, poprzez zastosowanie licencji, o funkcje inspekcji antywirusowej, inspekcji antyspamowej oraz filtrowania dostępu na podstawie adresów URL oraz reputacji strony internetowej.
23. Firewall musi posiadać możliwość rozbudowy, poprzez zastosowanie licencji, o mechanizm ochrony przed atakami 0-day na podstawie inspekcji sandbox realizowanej w chmurze obliczeniowej producenta.
24. Firewall musi posiadać możliwość rozbudowy, poprzez zastosowanie licencji o mechanizm umożliwiający pobieranie od producenta listy znanych adresów serwerów C&C (C2).
25. Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF, OSPFv3, IS-IS oraz BGP oraz wspierać Graceful Protocol Restart dla wymienionych. Urządzenie musi obsługiwać minimum 2 miliony prefiksów w tablicy RIB oraz 1,2 miliona prefiksów w tablicy FIB.
26. Urządzenie musi obsługiwać protokoły odpowiedzialne za przesyłanie ruchu multicastowego, w tym IGMPv2, PIM-SM, PIM-SSM oraz SDP, DMVRP oraz MSDP
27. Urządzenie musi posiadać funkcjonalność serwera DHCP.
28. Urządzenie musi posiadać 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.
29. Urządzenie musi posiadać możliwość tworzenia osobnych kolejek dla różnych klas ruchu, a kolejki muszą posiadać wsparcie dla mechanizmu WRED.
30. Urządzenie musi wspierać protokół MPLS i pozwalać na zestawianie połączeń MPLS L3VPN.
31. Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN z co najmniej 4000 znacznikami zgodnymi z 802.1Q.

32. Firewall musi pracować w konfiguracji odpornej na awarie opartej o klastrowanie urządzeń. Urządzenia połączone w klaster HA 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.
33. Firewall musi posiadać możliwość weryfikacji konfiguracji kandydackiej pod kątem zgodności i braku błędów przed jej zatwierdzeniem oraz możliwość automatycznego powrotu po jej zatwierdzeniu.
34. Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.
35. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.
36. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży na terenie Unii Europejskiej.
37. Sprzęt musi być fabrycznie nowy.

(support)

Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres 5 lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez wykonawcę lub polskiego partnera serwisowego, wymianę uszkodzonego sprzętu (wykonawca wysyła sprzęt następnego dnia roboczego), dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

(szkolenia)

Wymagane jest przeprowadzenie szkolenia z zakresu podstawowej konfiguracji i zarządzania urządzeniem przez wykonawcę lub autoryzowanego polskiego partnera serwisowego. Dopuszcza się szkolenie w formie videokonferencji. Szkolenie należy przeprowadzić najpóźniej 7 dni od dnia dostarczenia urządzeń

(migracja z istniejącego systemu)

Wymagane jest przeniesienie konfiguracji z istniejącego produkcyjnego systemu składającego się z dwóch urządzeń typu SRX5400 (klaster HA) na zakupione urządzenia zestawione w klaster HA.