Ogłoszenie nr 540149584-N-2019 z dnia 19-07-2019 r.

Moszczenica:

OGŁOSZENIE O ZMIANIE OGŁOSZENIA

OGŁOSZENIE DOTYCZY:

Ogłoszenia o zamówieniu

INFORMACJE O ZMIENIANYM OGŁOSZENIU

Numer: 573891-N-2019

Data: 15/07/2019

SEKCJA I: ZAMAWIAJĄCY

Gmina Moszczenica, Krajowy numer identyfikacyjny 59064794800000, ul. ul. Kosowska 1, 97-310 Moszczenica, woj. łódzkie, państwo Polska, tel. 446 169 570, e-mail Tomasz.Mikulski@moszczenica.pl, faks 446 169 625.

Adres strony internetowej (url): www.moszczenica.pl

SEKCJA II: ZMIANY W OGŁOSZENIU

II.1) Tekst, który należy zmienić:

Miejsce, w którym znajduje się zmieniany tekst:

Numer sekcji: II

Punkt: II.4)

W ogłoszeniu jest: 1. Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja fabrycznie nowego sprzętu IT w postaci przełączników oraz urządzenia firewall na potrzeby realizacji projektu pn.: Podniesienie atrakcyjności inwestycyjnej województwa łódzkiego poprzez kompleksowe uzbrojenie Moszczenickich Terenów Inwestycyjnych (MTI). 2. Wspólny Słownik Zamówień (CPV): 30230000-0 Sprzęt związany z komputerami 30200000-1 Urządzenia komputerowe 48000000-8 Pakiety oprogramowania i systemy informatyczne 32420000-3 Urządzenia sieciowe 32520000-4 Sprzęt i kable telekomunikacyjne 3.1. Przełączniki rdzeniowe – 2 szt. Elementem dostawy są dwa przełączniki rdzeniowe, optyczne, pracujące w standardzie 10Gb Ethernet, wraz z kompletem kabli umożliwiających połączenie w stos o następujących minimalnych parametrach każdy: Porty przełącznika: minimum 48*10G (SFP+), minimum 6*40G (QSFP+) z możliwością rozszycia każdego portu na 4x10G Stackowanie: możliwość połączenia minimum 4 przełączników w stos za pomocą portów SFP+ lub QSFP+ bez dedykowanego okablowania (wymagane dostarczenie okablowania typu DAC) Matryca przełączająca: 1440 Gb/s Przepustowość pakietów: minimum 1071 Mp/s (dla pakietów 64Kb) Pojemność tablicy MAC: minimum 96k (w trybie standard) / 32k (w trybie routee) / 288k (w trybie bridgee) wpisów Tablica routingu: minimum 8k (w trybie standard) / 128k (w trybie routee) / 8k (w trybie bridgee) wpisów Tablica ARP: minimum 208k (w trybie standard) / 16k (w trybie routee) / 16k (w trybie bridgee) wpisów Pamięć Flash: minimum 8GB Pamięć RAM: minimum 4GB Zasilanie urządzenia: minimum dwa modularne, w pełni redundantne zasilacze 230VAC, maksymalny pobór mocy przełącznika do 305W Chłodzenie urządzenia: aktywne, redundantne, minimum 4 wentylatory Certyfikaty bezpieczeństwa: CE, RoHS Ilość wpisów tablicy ACL: minimum 4k Ilość kolejek sprzętowych dla portów GE: minimum 8 Ilość aktywnych IEEE802.1Q VLAN: minimum 4094 Ruting L3: Ruting statyczny, RIPv1/v2, OSPFv2, RIPng, OSPFv3, BGP4+, Ruting LPM, Ruting PBR dla IPv4/IPv6, DVMRP, PIM-DM, PIM-SM, PIM-SSM, Static multicast route, pojemność tabeli routingu minimum 128k wpisów Obsługa VLAN: IEEE 802.1Q, QinQ, selektywne QinQ, elastyczne QinQ Wsparcie dla zdefiniowanych typów VLANów: MAC VLAN, Voice VLAN, PVLAN, Protocol VLAN, Multicast VLAN, N:1 VLAN Translation Obsługa protokołów IP: IPv6 oraz IPv4 Obsługa spanning tree: IEEE 802.1D STP, IEEE 802.1W RSTP, IEEE 802.1S MSTP, Root guard, BPDU guard, BPDU forwarding, BPDU tunnel Obsługa wirtualizacji: wirtualizacja z możliwością łączenia w stos urządzeń znajdujących się w oddalonych względem siebie lokalizacjach minimum do 50km Agregacja LACP: zgodne z IEEE 802.3ad, minimum 128 grup, minimum 8 portów per grupa, LACP Load Balance Inne funkcje L1 i L2: unicast/broadcast/multicast storm-control, GVRP DDM, UDLD, LLDP, LLDP-MED, Port Mirror, sFlow, Virtual Cable Testing Inne funkcje L3: VRRP, URPF, ECMP, BFD, VxLAN, IEEE VEPA, Trill, VSF Obsługa Openflow: Openflow 1.0 Funkcje QoS: SWRR, SP, WRR, DWRR, SDWRR, WRED, traffic shaping, klasyfikacja ruchu w oparciu o: CoS, ToS, DiffServ DSCP, ACL, port Bezpieczeństwo: Port, MAC based authentication, RADIUS, TACACS+, Guest VLAN, Auto VLAN, DHCP/DHCPv6 snooping, port security, IP source guard, ARP Guard, Local ARP Proxy, ARP binding, Anti ARP/NDP cheat, Anti ARP scan Listy kontroli dostępu: IP ACL, MAC ACL, IP-MAC ACL, time ranged ACL, VLAN based ACL, ACL konfigurowane na porcie lub VLANie Multicast: minimum 8000 grup multicastowych, IGMP v1/v2/v3, IGMP snooping, IGMP snooping fast leave, MLD snooping Zarządzanie: CLI, Web/SSL, Telnet, SSH, IPv4/IPv6 SNMP v1/v2c/v3, SNMP Trap, RMON 1,2,3,9, Dual firmware images/configuration files, 802.3ah Firmware oraz konfiguracja: oprogramowanie przełącznika (firmware) dostępny bez ograniczeń czasowych, przez cały okres cyklu życiowego urządzenia poprzez Internet, wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług, możliwość wgrania kilku plików z obrazem lub konfiguracją systemu, możliwość wgrania oprogramowania oraz konfiguracji poprzez TFTP/FTP, Obsługa DHCP: DHCP client/server/relay, DHCPv6 relay/server Rodzaj gwarancji: minimum 36 miesięcy, licząc od protokołu odbioru. Wymagane jest dostarczenie gwarancji producenta obejmującego także wsparcie techniczne na okres 36 miesięcy od podpisania protokołu odbioru. Wsparcie techniczne świadczone musi

być telefonicznie w języku polskim. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy. 3.2 Urządzenie firewall – 1 szt. Zamawiający wymaga dostarczenia urządzenia firewall zgodnego z poniższymi wymaganiami: Nr Wymagania minimalne 1. 1 Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance o wysokości maksymalnej 1U, przystosowane do montażu w szafie Rack 19". Całość sprzętu musi być zarządzana przez jednego producenta. 2. 2 Urządzenie musi być wyposażone w ☐ 4 interfejsy 10/100/1000 Ethernet (RJ45) ☐ 8 interfejsy 1GE SFP 3. 3 Urządzenie musi być wyposażone w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 200 MB. 4. 4 Urządzenie musi być wyposażone dedykowany port konsoli/zarządzania. Port ten musi być wydzielony co najmniej logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. 5. 5 Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 1 Gbps dla Firewall/kontroli aplikacji Minimum 750 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji Minimum 8.000 tys. nowych połączeń na sekundę Minimum 100.000 równoległych sesji 6. 6 Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy a. rutera (tzn. w warstwie 3 modelu OSI) b. przełącznika (tzn. w warstwie 2 modelu OSI) c. w trybie pasywnego nasłuchu (sniffer) d. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA) 7. 7 Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/wirtualna domena, itp.) 8. 8 Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3. 9. 9 Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa, tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk. 10. 10 Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN) 11. 11 Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Wydajność IPsec 400Mbps Minimum 500 tuneli IPSEC VPN Minumum 500 tuneli SSL VPN Remote Access Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 500 jednoczesnych użytkowników. 12. 12 Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach. a. Polityki definiujące powinny umożliwiać wykorzystanie i. adresów źródłowych ii. adresów docelowych iii. użytkowników iv. numerów portów usług v. kategorie URL b. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia i. RADIUS lub TACACS+ ii. LDAP iii. Kerberos lub SAML 2.0 13. 13 Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej ☐ oznaczania pakietów znacznikami DiffServ ☐ ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego ☐ utworzenia co najmniej 8 klas ruchu sieciowego ☐ kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników ☐ kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP ☐ przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego 14. 14 Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 15. 15 Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP. 16. 16 Urządzenie powinno mieć możliwość obsługi nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1. Wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych). 17. 17 Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu. 18. 18 Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active. 19. 19 Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 1.500 reguł polityki bezpieczeństwa. 20. 20 Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65.535 dostępnych portach tcp i udp. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych Urządzenie musi wykrywać co najmniej 2500 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 21. 21 Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana tylko jako „wartość" w polityce. 22. 22 Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. 23. 23 Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. 24. 24 Urządzenie musi pozwalać na analizę i blokowanie plików

przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji 25. 25 Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" 26. 26 Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. 27. 28 Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. 28. 29 Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: a) Microsoft Active Directory b) usługi katalogowe LDAP c) serwery Terminal Services 29. 30 Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana, nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. 30. 31 Urządzenie musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów, z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w urządzenie, który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników. 31. 32 Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 32. 33 Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń Moduł AV musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 33. 34 Urządzenie musi zapewniać ochronę przed atakami typu Spyware– Zamawiający dopuszcza, by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 34. 36 Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu botnet na podstawie analizy behawioralnej. 35. 37 Urządzenie musi posiadać funkcjonalność URL Flitering wraz z aktualizacją w okresie gwarancji. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. 36. 38 Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). 37. 39 System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą a. bazy lokalnej, b. serwera LDAP, c. RADIUS lub TACACS+ Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). 38. 40 Urządzenie musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI) 39. 41 Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. 40. 42 Urządzenie musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych 41. 43 Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG. 42. 45 Urządzenie musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się poprzez analizę heurystyczną Urządzenie musi pozwalać na blokowanie transmisji plików szyfrowanych co najmniej a. Dokumentów office (doc, xls, ppt) b. Plików skompresownych (zip, rar) Urządzenie musi posiadać funkcję automatycznego pobierania z zewnętrznych systemów adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty 43. 46 Urządzenie musi zapewniać wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym. Urządzenie musi posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora

systemu w tym. a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. b. Możliwość blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji Urządzenie musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w firewall i nie może wymagać korzystania z rozwiązań trzecich. Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Przywrócenie jednej z poprzednich wersji konfiguracji jako konfiguracji aktywnej nie może powodować konieczności restartu urządzenia 44. 47 W przypadku utraty komunikacji z centralną konsolą zarządzania urządzenie musi pozwalać na Lokalne zbieranie i analizowanie logów korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: a. ruchu sieciowym b. aplikacjach c. zagrożeniach d. filtrowaniu stron www tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Okres gwarancji dla urządzenia firewall wynosi minimum 36 miesięcy. Wymagane jest dostarczenie wsparcia producenta na okres 36 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie w języku polskim i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 8x5xNBD. 3.3 Usługa wsparcia technicznego: Wykonawca przeprowadzi prace instalacyjne i konfiguracyjne wspólnie z administratorami Zamawiającego w jego siedzibie. W ramach prac Wykonawca przekaże wiedzę dotyczącą realizowanej konfiguracji. Po przeprowadzeniu całości prac Wykonawca zapewni szkolenie dla maksymalnie 3 pracowników Zamawiającego w siedzibie Zamawiającego, które będzie obejmowało co najmniej: • Instalację dostarczonych urządzeń • Konfigurację urządzeń i włączenie ich do sieci Zamawiającego • Weryfikację konfiguracji w środowisku produkcyjnym • Backup i odtworzenie konfiguracji. Zamawiający na przedmiotową usługę wsparcia technicznego przewiduje 100 godzin (zegarowych). 3.4 Miejsce realizacji zamówienia Przedmiot zamówienia zostanie zrealizowany w budynku Moszczenickich Terenów Inwestycyjnych w Moszczenicy przy ul. Dworcowej 16. 3.5 Dokumentacja powykonawcza Wykonawca zobowiązany jest do opracowania i dostarczenia dokumentacji technicznej. Dokumentacja musi zawierać plan konfiguracji, implementacji oraz weryfikacji. Dokumentacja zostanie dostarczona na nośniku fizycznym (płyta CD/DVD) lub w formie elektronicznej na adres email podany przez Zamawiającego. Jeżeli w opisie przedmiotu zamówienia użyto nazw, znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę, ich zastosowanie nie jest obowiązkowe, zamawiający dopuszcza zastosowanie rozwiązań równoważnych, a nazwy zostały podane jedynie w celach informacyjnych dla umożliwienia porównania równoważności.

W ogłoszeniu powinno być: 1. Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja fabrycznie nowego sprzętu IT w postaci przełączników oraz urządzenia firewall na potrzeby realizacji projektu pn.: Podniesienie atrakcyjności inwestycyjnej województwa łódzkiego poprzez kompleksowe uzbrojenie Moszczenickich Terenów Inwestycyjnych (MTI). 2. Wspólny Słownik Zamówień (CPV): 30230000-0 Sprzęt związany z komputerami 30200000-1 Urządzenia komputerowe 48000000-8 Pakiety oprogramowania i systemy informatyczne 32420000-3 Urządzenia sieciowe 32520000-4 Sprzęt i kable telekomunikacyjne 3.1. Przełączniki rdzeniowe – 2 szt. Elementem dostawy są dwa przełączniki rdzeniowe, optyczne, pracujące w standardzie 10Gb Ethernet, wraz z kompletem kabli umożliwiających połączenie w stos o następujących minimalnych parametrach każdy: Porty przełącznika: minimum 48*10G (SFP+), minimum 6*40G (QSFP+) z możliwością rozszycia każdego portu na 4x10G Stackowanie: możliwość połączenia minimum 4 przełączników w stos za pomocą portów SFP+ lub QSFP+ bez dedykowanego okablowania (wymagane dostarczenie okablowania typu DAC) Matryca przełączająca: 1440 Gb/s Przepustowość pakietów: minimum 1071 Mp/s (dla pakietów 64Kb) Pojemność tablicy MAC: minimum 96k (w trybie standard) / 32k (w trybie routee) / 288k (w trybie bridgee) wpisów Tablica routingu: minimum 8k (w trybie standard) / 128k (w trybie routee) / 8k (w trybie bridgee) wpisów Tablica ARP: minimum 208k (w trybie standard) / 16k (w trybie routee) / 16k (w trybie bridgee) wpisów Pamięć Flash: minimum 8GB Pamięć RAM: minimum 4GB Zasilanie urządzenia: minimum dwa modularne, w pełni redundantne zasilacze 230VAC, maksymalny pobór mocy przełącznika do 305W Chłodzenie urządzenia: aktywne, redundantne, minimum 4 wentylatory Certyfikaty bezpieczeństwa: CE, RoHS Ilość wpisów tablicy ACL: minimum 4k Ilość kolejek sprzętowych dla portów GE: minimum 8 Ilość aktywnych IEEE802.1Q VLAN: minimum 4094 Ruting L3: Ruting statyczny, RIPv1/v2, OSPFv2, RIPng, OSPFv3, BGP4+, Ruting LPM, Ruting PBR dla IPv4/IPv6, DVMRP, PIM-DM, PIM-SM, PIM-SSM, Static multicast route, pojemność tabeli routingu minimum 128k wpisów Obsługa VLAN: IEEE 802.1Q, QinQ, selektywne QinQ, elastyczne QinQ Wsparcie dla zdefiniowanych typów VLANów: MAC VLAN, Voice VLAN, PVLAN, Protocol VLAN, Multicast VLAN, N:1 VLAN Translation Obsługa protokołów IP: IPv6 oraz IPv4 Obsługa spanning tree: IEEE 802.1D STP, IEEE 802.1W RSTP, IEEE 802.1S MSTP, Root guard, BPDU guard, BPDU forwarding, BPDU tunnel Obsługa wirtualizacji: wirtualizacja z możliwością łączenia w stos urządzeń znajdujących się w oddalonych względem siebie lokalizacjach minimum do 50km Agregacja LACP: zgodne z IEEE 802.3ad, minimum 128 grup, minimum 8 portów per grupa, LACP Load Balance Inne funkcje L1 i L2: unicast/broadcast/multicast storm-control, GVRP DDM, UDLD, LLDP, LLDP-MED, Port Mirror, sFlow, Virtual Cable Testing Inne funkcje L3: VRRP, URPF, ECMP, BFD, VxLAN, IEEE VEPA, Trill, VSF Obsługa Openflow: Openflow 1.0 Funkcje QoS: SWRR, SP, WRR, DWRR, SDWRR, WRED, traffic shaping, klasyfikacja ruchu w oparciu o: CoS, ToS, DiffServ DSCP, ACL, port Bezpieczeństwo: Port, MAC based authentication, RADIUS, TACACS+, Guest VLAN, Auto VLAN, DHCP/DHCPv6 snooping, port security, IP source guard, ARP Guard, Local ARP Proxy, ARP binding, Anti ARP/NDP cheat, Anti ARP scan Listy kontroli dostępu: IP ACL, MAC ACL, IP-MAC ACL, time ranged ACL, VLAN based ACL, ACL konfigurowane na porcie lub VLANie Multicast: minimum 8000 grup

multicastowych, IGMP v1/v2/v3, IGMP snooping, IGMP snooping fast leave, MLD snooping Zarządzanie: CLI, Web/SSL, Telnet, SSH, IPv4/IPv6 SNMP v1/v2c/v3, SNMP Trap, RMON 1,2,3,9, Dual firmware images/configuration files, 802.3ah Firmware oraz konfiguracja: oprogramowanie przełącznika (firmware) dostępny bez ograniczeń czasowych, przez cały okres cyklu życiowego urządzenia poprzez Internet, wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług, możliwość wgrania kilku plików z obrazem lub konfiguracją systemu, możliwość wgrania oprogramowania oraz konfiguracji poprzez TFTP/FTP, Obsługa DHCP: DHCP client/server/relay, DHCPv6 relay/server Rodzaj gwarancji: minimum 36 miesięcy, licząc od protokołu odbioru. Wymagane jest dostarczenie gwarancji producenta obejmującego także wsparcie techniczne na okres 36 miesięcy od podpisania protokołu odbioru. Wsparcie techniczne świadczone musi być telefonicznie w języku polskim. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy. 3.2 Urządzenie firewall – 1 szt. Zamawiający wymaga dostarczenia urządzenia firewall zgodnego z poniższymi wymaganiami: Nr Wymagania minimalne 1. 1 Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance o wysokości maksymalnej 1U, przystosowane do montażu w szafie Rack 19". Całość sprzętu musi być zarządzana przez jednego producenta. 2. 2 Urządzenie musi być wyposażone w ☐ 4 interfejsy 10/100/1000 Ethernet (RJ45) ☐ 8 interfejsy 1GE SFP 3. 3 Urządzenie musi być wyposażone w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 200 MB. 4. 4 Urządzenie musi być wyposażone dedykowany port konsoli/zarządzania. Port ten musi być wydzielony co najmniej logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. 5. 5 Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 1 Gbps dla Firewall/kontroli aplikacji Minimum 750 Mbps dla Firewall/IPS/Antywirus/kontroli aplikacji Minimum 8000 nowych połączeń na sekundę Minimum 100.000 równoległych sesji 6. 6 Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy a. rutera (tzn. w warstwie 3 modelu OSI) b. przełącznika (tzn. w warstwie 2 modelu OSI) c. w trybie pasywnego nasłuchu (sniffer) d. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA) 7. 7 Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/wirtualna domena, itp.) 8. 8 Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3. 9. 9 Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa, tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk. 10. 10 Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN) 11. 11 Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Wydajność IPsec 400Mbps Minimum 500 tuneli IPSEC VPN Minumum 500 tuneli SSL VPN Remote Access Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 500 jednoczesnych użytkowników. 12. 12 Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach. a. Polityki definiujące powinny umożliwiać wykorzystanie i. adresów źródłowych ii. adresów docelowych iii. użytkowników iv. numerów portów usług v. kategorie URL b. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia i. RADIUS lub TACACS+ ii. LDAP iii. Kerberos lub SAML 2.0 13. 13 Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej ☐ oznaczania pakietów znacznikami DiffServ ☐ ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego ☐ utworzenia co najmniej 8 klas ruchu sieciowego ☐ kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników ☐ kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP ☐ przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego 14. 14 Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 15. 15 Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP. 16. 16 Urządzenie powinno mieć możliwość obsługi nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1. Wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych). 17. 17 Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu. 18. 18 Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active. 19. 19 Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 1.500 reguł polityki bezpieczeństwa. 20. 20 Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65.535 dostępnych portach tcp i udp. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych Urządzenie musi wykrywać

co najmniej 2500 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 21. 21 Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana tylko jako „wartość" w polityce. 22. 22 Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. 23. 23 Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. 24. 24 Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji 25. 25 Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" 26. 26 Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. 27. 28 Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. 28. 29 Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: a) Microsoft Active Directory b) usługi katalogowe LDAP c) serwery Terminal Services 29. 30 Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana, nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. 30. 31 Urządzenie musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów, z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w urządzenie, który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników. 31. 32 Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 32. 33 Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń Moduł AV musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 33. 34 Urządzenie musi zapewniać ochronę przed atakami typu Spyware– Zamawiający dopuszcza, by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. 34. 36 Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu botnet na podstawie analizy behawioralnej. 35. 37 Urządzenie musi posiadać funkcjonalność URL Flitering wraz z aktualizacją w okresie gwarancji. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. 36. 38 Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). 37. 39 System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą a. bazy lokalnej, b. serwera LDAP, c. RADIUS lub TACACS+ Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). 38. 40 Urządzenie musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI) 39. 41 Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji

konfiguracji na dysku twardym urządzenia. 40. 42 Urządzenie musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall /kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych 41. 43 Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG. 42. 45 Urządzenie musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się poprzez analizę heurystyczną Urządzenie musi pozwalać na blokowanie transmisji plików szyfrowanych co najmniej a. Dokumentów office (doc, xls, ppt) b. Plików skompresownaych (zip, rar) Urządzenie musi posiadać funkcję automatycznego pobierania z zewnętrznych systemów adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty 43. 46 Urządzenie musi zapewniać wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym. Urządzenie musi posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu w tym. a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. b. Możliwość blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji Urządzenie musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w firewall i nie może wymagać korzystania z rozwiązań trzecich. Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Przywrócenie jednej z poprzednich wersji konfiguracji jako konfiguracji aktywnej nie może powodować konieczności restartu urządzenia 44. 47 W przypadku utraty komunikacji z centralną konsolą zarządzania urządzenie musi pozwalać na ☐ Lokalne zbieranie i analizowanie logów ☐ korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: a. ruchu sieciowym b. aplikacjach c. zagrożeniach d. filtrowaniu stron www ☐ tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. ☐ tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Okres gwarancji dla urządzenia firewall wynosi minimum 36 miesięcy. Wymagane jest dostarczenie wsparcia producenta na okres 36 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie w języku polskim i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 8x5xNBD. 3.3 Usługa wsparcia technicznego: Wykonawca przeprowadzi prace instalacyjne i konfiguracyjne wspólnie z administratorami Zamawiającego w jego siedzibie. W ramach prac Wykonawca przekaże wiedzę dotyczącą realizowanej konfiguracji. Po przeprowadzeniu całości prac Wykonawca zapewni szkolenie dla maksymalnie 3 pracowników Zamawiającego w siedzibie Zamawiającego, które będzie obejmowało co najmniej: • Instalację dostarczonych urządzeń • Konfigurację urządzeń i włączenie ich do sieci Zamawiającego • Weryfikację konfiguracji w środowisku produkcyjnym • Backup i odtworzenie konfiguracji. Zamawiający na przedmiotową usługę wsparcia technicznego przewiduje 100 godzin (zegarowych). 3.4 Miejsce realizacji zamówienia Przedmiot zamówienia zostanie zrealizowany w budynku Moszczenickich Terenów Inwestycyjnych w Moszczenicy przy ul. Dworcowej 16. 3.5 Dokumentacja powykonawcza Wykonawca zobowiązany jest do opracowania i dostarczenia dokumentacji technicznej. Dokumentacja musi zawierać plan konfiguracji, implementacji oraz weryfikacji. Dokumentacja zostanie dostarczona na nośniku fizycznym (płyta CD/DVD) lub w formie elektronicznej na adres email podany przez Zamawiającego. Jeżeli w opisie przedmiotu zamówienia użyto nazw, znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę, ich zastosowanie nie jest obowiązkowe, zamawiający dopuszcza zastosowanie rozwiązań równoważnych, a nazwy zostały podane jedynie w celach informacyjnych dla umożliwienia porównania równoważności.

Miejsce, w którym znajduje się zmieniany tekst:

Numer sekcji: IV

Punkt: IV.6.2)

W ogłoszeniu jest: Termin składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu: Data: 2019-07-23, godzina: 10:00

W ogłoszeniu powinno być: Termin składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu: Data: 2019-07-24, godzina: 10:00

Z up. WÓJTA GMINY

Krzysztof Jędrzejczyk
SEKRETARZ GMINY