OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ 1 - DOSTAWA URZĄDZEŃ DO SERWEROWNI
KOD CPV: 30200000-1

1. System zabezpieczeń sieciowych (Firewall) UTM - 1 szt.

Właściwości systemu zabezpieczeń sieciowych UTM (Unified Threat Management):

1. System zabezpieczeń musi realizować zadania firewall, wykonując kontrolę na poziomie sieci oraz aplikacji Urządzenie musi realizować zarządzanie pasmem sieci (QoS) oraz musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site.

2. Urządzenie zabezpieczeń musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS) wspieranego sprzętowo. Aktualizacja bazy sygnatur ataków (IPS) powinna odbywać się na żądanie, bądź automatycznie zgodnie z ustalonym w konfiguracji harmonogramem.

3. Urządzenie zabezpieczeń musi posiadać możliwość uruchomienia modułu kontroli antywirusowej kontrolującego pocztę elektronicznej (SMTP, POP3, IMAP, FTP oraz HTTP. Włączenie kontroli antywirusowej nie wymaga dodatkowego serwera.

4. Urządzenie zabezpieczeń musi posiadać możliwość uruchomienia modułu kontroli antyspamowej działającego w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie wymaga dodatkowego serwera.

5. Urządzenie zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie wymaga dodatkowego serwera.

6. System zabezpieczeń musi być dostarczany jako dedykowane urządzenie sieciowe nie posiadające wrażliwych na awarie elementów sprzętowych (np. twardego dysku). Całość sprzętu i oprogramowania musi być dostarczana i supportowana przez jednego producenta.

7. System zabezpieczeń nie może posiadać ograniczeń na liczbę chronionych komputerów w sieci wewnętrznej.

8. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki definiowane są pomiędzy dowolnymi strefami bezpieczeństwa. Urządzenie musi obsługiwać nie mniej niż 12 stref bezpieczeństwa.

9. Urządzenie zabezpieczeń musi być sterowane przez opracowany przez producenta zabezpieczeń dedykowany system operacyjny.

10. Urządzenie zabezpieczeń musi posiadać przepływność firewall nie mniej niż 750 Mbps (dla dużych pakietów) i nie mniej niż 250 Mb/s dla ruchu dla ruchu IMIX; nie mniejszą niż 75 Mb/s dla IPSec VPN (3DES/AES) i obsługiwać nie mniej niż 500 polityk bezpieczeństwa.

11. Urządzenie zabezpieczeń musi być wyposażone w 2 porty Gigabit Ethernet 10/100/1000 Base-T i 6 portów 10/100 Base-T Ethernet oraz posiadać slot na dodatkowe moduły interfejsów. Wbudowane interfejsy muszą umożliwić dowolne definiowanie trybu pracy – jako interfejs L3, czy też grupowanie interfejsów w grupę L2 (Bridge Group).

12. W urządzeniu musi istnieć możliwość uruchomienia następujących interfejsów sieciowych: E1, Serial, ISDN BRI, ADSL2, oraz Ethernet 1000 Mbps SFP.

13. Urządzenie musi zapewniać obsługę 64 sieci VLAN

14. Urządzenie musi posiadać minimum 1 GB pamięci operacyjnej (DRAM).

15. Sieci VPN tworzone przez system zabezpieczeń muszą działać poprawnie w środowiskach sieciowych, gdzie na drodze VPN wykonywana jest translacja adresów NAT. System zabezpieczeń musi posiadać zaimplementowany mechanizm IPSec NAT Traversal dla konfiguracji VPN client-to-site oraz site-to-site.

16. System zabezpieczeń musi posiadać zaimplementowane mechanizmy monitorowania stanu tuneli VPN i stałego utrzymywania ich aktywności (tzn. po wykryciu nieaktywności tunelu automatycznie następuje negocjacja IKE).

17. Konfiguracja VPN musi odbywać się w oparciu o reguły polityki bezpieczeństwa (Policy-based VPN) oraz ustawienia rutingu (Routing-based VPN).

18. Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych ruterów posiadających odrębne tabele rutingu, umożliwiające podłączenie do urządzenia sieci o tej samej adresacji IP. Urządzenie musi obsługiwać protokoły rutingu RIP, OSPF i BGP.

19. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).

20. Zarządzanie funkcjami zabezpieczeń w pełnym zakresie musi odbywać się z linii poleceń (CLI), graficznej konsoli GUI, oraz scentralizowanego systemu zarządzania. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Administratorzy mogą być uwierzytelniani za pomocą haseł statycznych oraz haseł dynamicznych (RADIUS)

21. System zabezpieczeń musi posiadać mechanizmy uwierzytelniania tożsamości użytkowników za pomocą haseł statycznych i dynamicznych. Użytkownicy definiowani są w bazie lokalnej (tzn. bazie utrzymywanej na urządzeniu) oraz na zewnętrznych serwerach LDAP, RADIUS lub SecurID (ACE/Server).

22. System zabezpieczeń musi współpracować z wiodącymi urzędami certyfikacji (m.in. Verisign, Entrust, Microsoft) i musi wspierać standardy PKI (PKCS 7, PKCS 10) oraz protokół SCEP

23. System zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT umożliwiają m.in. dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. Udostępnianie w Internecie usług wielu serwerów musi odbywać się z użyciem tylko jednego publicznego adresu IP.

24. System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

25. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.

26. Wraz z produktem wymagane jest dostarczenie opieki technicznej oraz subskrypcji na funkcję IPS (AV, AS etc) ważnej przez okres X lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora zabezpieczeń, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację bazy ataków IPS, definicji wirusów, blacklist antyspamowych oraz bazy kategorii stron WWW, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych

Powyższe wymagania spełnia np. urządzenie: Juniper SRX 210

2. Przełącznik dostępowy (switch) – 2 szt

1. Przełącznik o zamkniętej konfiguracji, posiadający 48 porty uniwersalne GigaEthernet 10/100/1000 oraz 4 gniazda typu SFP pozwalające na instalację wkładek z portami Gigabit Ethernet 1000BASE-T, 1000BASE-SX, 1000BASE-ZX, 1000BASE LX/LH

2. Przełącznik musi posiadać co najmniej 128 MB pamięci DRAM oraz 32 MB pamięci Flash

3. Dostępne w przełączniku gniazda SFP powinny umożliwiać instalację modułów dla zwielokrotnionej transmisji optycznej CWDM

4. Przełącznik musi posiadać wydajność przełączania przynajmniej 38 Mpps dla 64-bajtowych pakietów;

5. Przełącznik musi zapewniac obsługę 12,000 adresów MAC, 11,000 tras w tablicy routingu, 1024 sieci VLAN oraz 128 instancji STP

6. Przełącznik musi współpracować z modułem redundantnego zewnętrznego zasilacza.

7. Przełącznik musi zapewniać przełączanie w warstwie drugiej,

8. Przełącznik musi w standardowej wersji oprogramowania umożliwiać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1/v2 oraz routing statyczny

9. Przełącznik musi posiadać możliwość rozszerzenia funkcjonalności routingu o obsługę protokołów EIGRP, OSPF i BGPv4, poprzez wymianę oprogramowania.

10. Przełącznik musi zapewniać podstawową obsługę ruchu IP Multicast, w tym funkcjonalność IGMP oraz IGMP Snooping.

11. Przełącznik musi posiadać możliwość rozszerzenia funkcjonalności IP Multicast o obsługę protokołów PIM Sparse oraz PIM Dense, poprzez wymianę oprogramowania.

12. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server oraz DHCP Relay

13. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

a. IEEE 802.1s Rapid Spanning Tree

b. IEEE 802.1w Multi-Instance Spanning Tree

c. możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP)

14. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości

usług w sieci:

a. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, żródłowy/docelowy port TCP

b. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek

c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)

d. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.

e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Dla portu GigaEthernet 10/100/1000 wymagana możliwość skonfigurowania co najmniej 64 różnych ograniczeń, każde odpowiednio dla różnej klasy obsługi ruchu

15. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

a. Wiele poziomów dostępu administracyjnego poprzez konsolę

b. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x oraz EAP

c. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2

d. Poprzez wymianę oprogramowania uzupełnienie o funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym

16. Przełącznik powinien umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu

17. Przełącznik powinien umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN

18. Przełącznik powinien miec możliwość synchronizacji zegara czasu za pomocą protokołu NTP

19. Urządzenie powinno umożliwiać zarządzania poprzez interfejs CLI (konsolę).

20. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) powinien byc możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po

zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 4 plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu

21. Musi mieć możliwość montażu w szafie 19", wysokość nie większą niż 1RU;

22. Możliwość podłączenia zewnętrznego źródła zasialania, które w przypadku awarii wewnęrznego zasialacza, dostarczy wymagany przez urządzenie poziom zasilania bez przerw w pracy sieci.

Powyższe wymagania spełnia urządzenie: Cisco WS-C3560G-48TS-S

3. Zasilacz awaryjny UPS

1. Moc wyjściowa - 2700W / 3000 VA

2. Maksymalna moc, jaką można skonfigurować - 2700W / 3000 VA

3. Napięcie wyjściowe - 230V

4. Napięcie wyjściowe konfigurowalne dla 220 : 230 lub 240 napięcia wyjściowego

5. Zniekształcenia napięcia wyjściowego mniej niż 5% przy pełnym obciążeniu

6. Częstotliwość na wyjściu (synchronicznie z siecią) tj. 47–53 Hz przy częstotliwości nominalnej 50 Hz,57–63 Hz przy częstotliwości nominalnej 60 Hz

7. Typ przebiegu - sinusoida

8. Gniazda wyjściowe 8 x IEC 320 C13, 1 x IEC 320 C19

9. Nominalne napięcie wejściowe 230V

10. Częstotliwość na wejściu 50/60 Hz +/- 3% (autodetekcja)

11. Typ gniazda wejściowego IEC-320 C20

12. Zakres napięcia wejściowego w trybie podstawowym 160 - 286V

13. Zmienny zakres napięcia wejściowego w trybie podstawowym 151 - 302V

14. Typ akumulatora Bezobsługowe baterie ołowiowo-kwasowe

15. Typowy czas pełnego ładowania akumulatora 3 godziny

16. Port komunikacyjny DB-9 RS-232,Gniazdo typu SmartSlot,USB

17. Ilość interfejsów SmartSlot 1

18. Panel przedni: Diody LED wskazują stan obciążenia, stan prac z sieci, prace z baterii, stan wymiany baterii, stan przeciążenia

19. Alarm dźwiękowy podczas pracy na baterii: znaczny stan wyczerpania baterii, ustawialne przez użytkownika opóźnienia

20. Awaryjny wyłącznik zasilania

21. Filtracja Full time multi-pole noise filtering : 0.3% IEEE surge let-through : zero clamping response time : meets UL 1449

22. Wysokość w szafie przemysłowej 2U

23. Maksymalna wysokość 89.00 mm

24. Maksymalna szerokość 483.00 mm

25. Maksymalna głębokość 660.00 mm

26. Środowisko operacyjne 0 - 40 °C

27. Wilgotność względna podczas pracy 0 - 95%

28. Automatyczna regulacja napięcia (AVR) z funkcją korekcji niskich i wysokich napięć.

29. Inteligentne zarządzanie bateriami

30. Filtrowanie napięcia Chroniące podłączone obciążenia przed przepięciami, impulsami elektrycznymi, uderzeniami pioruna i innymi zakłóceniami zasilania.

31. Ładowanie akumulatorów dostosowane do temperatury np. Wydłużenie czasu eksploatacji akumulatorów przez regulację napięcia ładowania w zależności od temperatury akumulatora.

32. Automatyczne włączenie UPS-a po powrocie zasilania

33. Automatyczny okresowy autotest akumulatora zapewniające wczesne wykrywanie konieczności wymiany.

34. Możliwość zimnego startu

35. Powiadomienie o rozłączeniu akumulatora

36. Zarządzanie zdalne umożliwia zarządzanie UPS-em przez sieć.

37. Zarządzanie zasilaczem UPS przez port szeregowy.

38. Zarządzanie UPS-em przez port USB.

39. Powiadomienie o rozłączeniu akumulatora

Powyższe wymagania spełnia urządzenie: UPS APC SUA3000RMI2U

4. Karta do monitorowania urządzenia UPS oraz zmiennych środowiskowych

1. Protokoły: HTTP,HTTPS,SMTP,SNMP,SSL,TCP/IP,Telnet,WAP

2. Połączenia interfejsów sieciowych RJ-45 10/100 Base-T

3. Zaciski wejściowe do monitorowanie warunków z urządzeń zewnętrznych.

4. Monitorowanie wilgotności. Zmiany wilgotności są zgłaszane przez interfejs użytkownika lub pocztą e-mail.

5. Monitorowanie temperatury. Zmiany temperatury są zgłaszane przez interfejs użytkownika lub pocztą e-mail.

6. Dostosowywane przekaźniki sterujące/ wyjściowe. Sterowanie wyjściami z urządzeń zewnętrznych firm przez przekaźniki wyjściowe.

7. Powiadamianie o problemach gwarantujące szybkie reagowanie na sytuacje wymagające interwencji.

8. Definiowalne przez użytkownika parametry pozwalają na zamknięcie podłączonego sprzętu lub UPSów jeśli jest to konieczne.

9. Ustalone działania w odpowiedzi na zaistniałe zdarzenia dotyczące zasilania.

10. Identyfikacja niepokojących objawy zanim zaczną stanowić problem lub wyeksportuj logi danych dla analizy.

11. Dostęp przez przeglądarkę. Możliwość szybkiego dostępu z dowolnego miejsca w sieci

12. Oprogramowanie sprzętowe w pamięci flash z możliwością uaktualniania przy użyciu FTP.

13. Zabezpieczenie hasłem

14. Trzy poziomy dostępu użytkowników: tylko odczyt, poziom urządzenia i administracyjny.

15. Obsługa standardu Radius

16. Kompatybilne z zasilaczami UPS wyposażonymi w gniazdo Smart-Slot

Powyższe wymagania spełnia urządzenie: APC AP9618

5. Urządzenie do dystrybucji zasilania

1. Napięcie wyjściowe 208V,230V

2. Maksymalny całkowity pobór prądu 16A

3. Gniazda wyjściowe 8 x IEC 320 C13

4. Nominalne napięcie wejściowe 200V,208V,230V

5. Częstotliwość na wejściu 50/60 Hz

6. Prąd wejściowy - 16A

7. Typ gniazda wejściowego IEC-320 C20

8. Długość przewodu zasilania min 2.5 metry

9. Ilość kabli zasilających 1

10. Tolerancja napięcia wejściowego 200-240 VAC

11. Maksymalny prąd na wejściu 20A

12. Poziom obciążenia 3680 VA

13. Wysokość w szafie teletechnicznej - 1U

14. Pełnowymiarowe interfejsy do zarządzania sieciowego zapewniające oparte na standardach zarządzanie przez sieć, SNMP i Telnet.

15. Możliwość szybkiej i łatwej aktualizacji oprogramowania sprzętowego przez sieć.

16. Zdalne zarządzani wyjściami.

17. Ogólny pobór mocy przez urządzenie rozdziału zasilania jest ukazany na wyświetlaczu urządzenia.

18. Umożliwia użytkownikom skonfigurowanie kolejności włączania i wyłączania zasilania w poszczególnych wyjściach. Pomaga to uniknąć kumulacji momentu rozruchowego przy starcie urządzeń, który może być przyczyną przeciążenia obwodu i odłączenie obciążeń.

19. Wskaźnik obciążenia LED Informuje i przeciążeniu i warunkach zagrożenia na podstawie zdefiniowanych przez użytkownika progów alarmowych. □

Powyższe wymagania spełnia urządzenie: APC AP7921

6. Szafa rack 42U z wyposażeniem

1. Szerokość: 800mm

2. Głębokość: 1200mm

3. Wysokość: 1963mm (42U)

4. Drzwi przednie szklane

5. Drzwi tylne blaszane z perforacją drobną

6. Osłony boczne z perforacją drobną

7. Cokół o wysokości 100mm

8. W cokole powinna być zamontowana wysuwana rama wsporcza

9. Tylna ściana cokołu powinna posiadać przepust szczotkowy

10. Boczne ściany cokołu powinny być pełne (bez perforacji)

11. W szafie powinny być zamontowane dwie pary belek nośnych 19" oraz jedna para belek nośnych środkowych

12. Kolor - czarny

13. Szafa powinna być wyposażona w panel wentylatorów z termostatem

14. W szafie powinny być zamontowane 2 szt półek

15. Jeden panel zasilająco-filtrujący 19”/2U (5 gniazd 220V/10A)

Powyższe wymagania spełnia: ZPAS WZ-SZBSE-25-3422-13-7411-1-161