Część II SIWZ

Szczegółowy Opis Przedmiotu Zamówienia

I. Wstęp

Zadanie obejmuje dostawę 2 przełączników dostępowych 24 portowych z POE, 5 przełączników dostępowych 48 portowych z POE oraz dwóch urządzeń typu Firewall, wraz z techniczną infrastrukturą towarzyszącą (wyposażenia sfp, sfp+, patchordy, kable zasilające do urządzeń, elementy montażowe w szafach Rack). Powyższe urządzenia należy dostarczyć, przeprowadzić szkolenie, zainstalować oraz skonfigurować w ramach posiadanej przez zamawiającego infrastruktury sieciowej.

Zamawiający wymaga, aby sprzęt aktywny (wraz z dedykowanymi akcesoriami) pochodził z legalnego kanału dystrybucji producenta. Zamawiający wymaga, aby sprzęt był fabrycznie nowy, nieużywany i nie stanowił części projektu dla innego klienta na terenie Unii Europejskiej. Dopuszcza się urządzenia pochodzące spoza granic Polski pod warunkiem, że będą spełniały wszystkie normy i przepisy wymagane na terenie Polski oraz są dedykowane na rynek polski.

Zamawiający wymaga aby wykonawca przedstawił opinie producenta sprzętu, że wykonawca jest oficjalnym partnerem proponowanego do zakupu sprzętu, a sprzęt przewidziany jest w dystrybucji na rynek polski.

Przełączniki dostępowe 24 portowe mają tworzyć jedną, jednolitą strukturę logiczną (stack lub podobną) z ruchem miedzy przełącznikami w tej strukturze zestawionym o przepustowości minimum 10G. Każdy z przełączników ma umożliwiać lokalne przełączanie ruchu.

Wymagane jest aby każdy z przełączników dostępowych został podłączony do przełączników rdzeniowych (Brocate VDX 6740, posiadane przez zamawiającego) w sposób redundantny z agregacją łącza o przepustowości nie mniejszej niż 20G. Wymagane zestawienie minimum 2 linków, każdy do innego przełącznika rdzeniowego.

Przełączniki 24 portowe powinny mieć zapewnione podwójne zasilanie (dwa zasilacze lub zasilanie redundantne). Budżet mocy dla przełączników 24 portowych wynosi 370W a dla 48 portowych 740W. W lokalizacji dla przełączników 24 portowych zamawiający posiada dostępne zasilanie redundantne w postaci urządzenia Brocade ICX-EPS4000 oraz do dyspozycji dwa nieobsadzone zasilacze RPS17 (920W) wraz z okablowaniem (ICX-EPS4000-CBL-02). Na chwilę obecna do zasilania redundantnego podłączone są dwa przełączniki Brocade ICX7250-48P przy wykorzystaniu dwóch zasilaczy RPS17.

Wymagane jest aby przełączniki dostępowe zostały podłączone do posiadanego przez zamawiającego oprogramowania do zarządzania i monitoringu sieci (Brocade Network Advisor), przy zapewnieniu pełnej funkcjonalności lub w przypadku dostarczenia innego rozwiązania do zarządzania, zapewnienie pełnej funkcjonalności dla posiadanej przez zamawiającego infrastruktury sieciowej (sieć SAN, Brocade VDX6740, ICX7250, VMware vCenter).

II. Wymagania technicznie dla 24 portowych przełączników dostępowych.

1. Architektura
   - Urządzenie przystosowane do montażu w stelażu 19 cali, o wysokości 1U.
   - Minimum 24 portów 10/100/1000Mbps RJ-45.
   - Minimum 8 portów uplink 10Gbps na wkładki SFP+
   - Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management (Ethernet RJ-45).
   - Przełącznik musi posiadać port USB wspierający transfer plików do i z przełącznika

- Całkowita wydajność przełączania min. 208 Gbps, 154 Mpps.
- Całkowita wydajność prądowa wbudowanego pojedynczego zasilacza musi zapewniać zasilenie wszystkich 24 portów w trybie PoE (802.3at klasa 3).
- Całkowita wydajność prądowa zasilacza wbudowanego i zewnętrznego musi zapewniać zasilenie wszystkich 24 portów w trybie PoE+ (30W per port)

2. Funkcjonalność łączenia w stos
   - Możliwość stackowania minimum 12 urządzeń w jednym stosie na odległość do 10km.
   - Minimalna przepustowość połączeń w stosie 20Gbps (stackowanie po dwóch portach 10Gps per przełącznik)
   - Obsługa trybu Hitless Failover w przypadku awarii przełącznika typu master w stosie.

3. Funkcjonalność warstwy II
   - Urządzenie musi obsługiwać min. 15000 adresów MAC oraz min. 4000 sieci VLAN.
   - Urządzenie musi posiadać min. 2GB pamięci DRAM i 1GB pamięci flash
   - Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad (LACP), min. 8 portów na jedno logiczne połączenie, min. 124 logicznych grup połączeń jednocześnie (w stosie).
   - Wsparcie dla RSTP oraz, 802.1s – Multiple Spanning Tree oraz PVST/PVST+/PVRST.
   - Obsługa do 254 instancji STP
   - Wsparcie dla 802.1x.
   - Możliwość uwierzytelniania użytkowników w oparciu o portal www (WebAuth)
   - Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection
   - Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server oraz wspierać funkcję DHCP Helper
   - Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP)) - protokół wykrywający sąsiednie urządzenia i ich atrybuty.
   - Wsparcie dla pakietów tzw. „Jumbo frames" (9216 bajtów).
   - Obsługa BPDU Guard, Root Guard.
   - Obsługa mechanizmu GVRP.
   - Obsługa IGMP snooping v1, v2, v3.
   - Obsługa Dynamic Voice VLAN Assignment.
   - Obsługa Link Fault Signaling (LFS) lub podobny.
   - Obsługa mechanizmu MAC Address Locking, Port Security.
   - Obsługa MLD Snooping (v1/v2).
   - Obsługa Multi-device Authentication.
   - Obsługa Mirroring - Port-based, ACL-based, MAC Filter-based, and VLAN-based.
   - Obsługa Port Loop Detection
   - Obsługa Private VLAN
   - Obsługa Protected Link Groups
   - Obsługa Protocol VLAN (802.1v), Subnet VLAN
   - Obsługa Remote Fault Notification (RFN).
   - Obsługa Single-instance Spanning Tree.
   - Obsługa Single-link LACP.
   - Obsługa Uni-Directional Link Detection (UDLD).
   - Obsługa Metro-Ring Protocol v1, v2.
   - Obsługa QinQ

4. Obsługa mechanizmów warstwy III
   - Statyczny routing IPv4 i IPv6.
   - Sprzętowa obsługa do 12000 wpisów routingu dla IPv4 oraz 1000 dla IPv6
   - Wsparcie tras ECMP.

5. Obsługa protokołów routingu dynamicznego
   - Obsługa protokołu RIPv2
   - Obsługa protokołu OSPFv2
   - Obsługa protokołu VRRP.
   - Obsługa protokołu GRE.
   - Obsługa protokołu BGP
6. Mechanizmy bezpieczeństwa
   - Obsługa zarówno IPv4 ACL jak i IPv6 ACL.
   - Możliwość konfiguracji mirroringu w oparciu o dany port, listy ACL i MAC, oraz VLAN.
   - Obsługa Private Vlan.
   - Obsługa DHCP snooping
   - Obsługa Dynamic ARP inspection
   - Obsługa Authentication, Authorization, and Accounting (AAA)
   - Wsparcie dla Advanced Encryption Standard (AES) i SSHv2
   - Obsługa RADIUS/TACACS/TACACS+
   - Obsługa Secure Copy (SCP) i Secure Shell (SSHv2)
   - Obsługa Change of Authorization (CoA) RFC 5176
7. Mechanizmy QoS
   - Obsługa 8 kolejek QoS na jednym porcie fizycznym.
   - Zarządzanie polityką jakości ruchu – "QoS" w oparciu o algorytmy Weighted Round Robin (WRR), Strict Priotity (SP) i ich kombinację.
   - Mapowanie za pomocą ACL do kolejki priorytetowej.
   - Mapowanie do kolejki priorytetowej na podstawie adresu MAC.
   - Limitowanie pasma na wejściu w oparciu o port, ACL.
   - Limitowanie pasma na wyjściu w oparciu o port, kolejkę.
   - Limitowanie pasma dla pakietów BUM (Broadcast, multicast i unknown unicast).
   - Obsługa Diffserv oraz DSCP/802.1p.
8. Inne
   - Obsługa SNMP2/SNMP3 oraz uwierzytelnianie poprzez TACACS/Radius.
   - Obsługa przez wbudowany serwer WWW.
   - Obsługa DHCP Server.
   - Obsługa DHCP Relay.
   - Obsługa NTP Network Time Protocol.
   - Obsługa 802.3az-2010 – EEE.
   - Musi być obsługiwana funkcja WriteNet - dzięki której przełącznik wykona upload swojego pliku konfiguracyjnego na zdalny serwer TFTP/SCP po otrzymaniu odpowiednich pakietów SNMP Write. Musi istnieć dodatkowe zabezpieczenie tej funkcji hasłem (np. enable) lub możliwość definiowana listy zaufanych serwerów TFTP/SCP.
   - Plik konfiguracyjny urządzenia musi być 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 nową konfiguracją.
9. Zgodność ze standardami
   - RFC 783 TFTP
   - RFC 854 TELNET Client and Server
   - RFC 951 Bootp
   - RFC 1157 SNMPv1/v2c
   - RFC 1213 MIB-II
   - RFC 1493 Bridge MIB
   - RFC 1516 Repeater MIB
   - RFC 1573 SNMP MIB II

- RFC 1643 Ethernet Interface MIB
- RFC 1724 RIP v1/v2 MIB
- RFC 1757 RMON MIB
- RFC 2068 Embedded HTTP
- RFC 2131 DHCP Server and DHCP Relay
- RFC 2570 SNMPv3 Intro to Framework
- RFC 2571 Architecture for Describing SNMP Framework
- RFC 2572 SNMP Message Processing and Dispatching
- RFC 2573 SNMPv3 Applications
- RFC 2574 SNMPv3 User-based Security Model
- RFC 2575 SNMP View-based Access Control Model SNMP
- RFC 2818 Embedded HTTPS
- RFC 3176 sFlow
- 802.1D-2004 MAC Bridging
- 802.1p Mapping to Priority Queue
- 802.1s Multiple Spanning Tree
- 802.1w Rapid Spanning Tree (RSTP)
- 802.1x Port-based Network Access Control
- 802.3 10Base-T
- 802.3ab 1000Base-T
- 802.3ad Link Aggregation (Dynamic and Static)
- 802.3ae 10 Gigabit Ethernet
- 802.3af Power over Ethernet
- 802.3at Power over Ethernet Plus
- 802.3u 100Base-TX
- 802.3x Flow Control
- 802.3z 1000Base-SX/LX
- 802.3 MAU MIB (RFC 2239)
- 802.3az-2010 – EEE
- 802.1Q VLAN Tagging

III. Wymagania technicznie dla 48 portowych przełączników dostępowych.

1. Typ i liczba portów liniowych w ramach urządzenia:
   - Minimum 48 portów 10/100/1000 PoE+ zgodne z IEEE 802.3af oraz 802.3at
   - Minimum 6 portów 1GE SFP
   - Minimum 2 porty stack o wydajności minimum 10Gbps każdy.
   - Wszystkie porty liniowe muszą być z przodu obudowy. Porty stack mogą znajdować się z tyłu obudowy.
   - Musi istnieć możliwość upgrade portów 1GE SFP na porty 10GE SFP poprzez wymianę karty 4xSFP lub instalację odpowiedniej licencji. Porty po aktualizacji muszą wpierać prędkość 1G lub 10G w zależności od zainstalowanej wkładki SFP lub SFP+.
   - Porty 1GE (SFP) muszą umożliwiać ich obsadzanie wkładkami – minimum 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U zależnie od potrzeb Zamawiającego
2. Wymagane jest, aby wszystkie porty dostępowe 10/100/1000 obsługiwały standard zasilania poprzez sieć LAN (Power over Ethernet) zgodnie ze standardami IEEE 802.3af IEEE 802.3at. Budżet mocy PoE/PoE+ musi wystarczyć na jednoczesne zasilenie 24 portów 10/100/1000 z wykorzystaniem klasy 4 PoE+ (30W per 1 port) lub jednoczesne zasilenie 48 portów 10/100/1000 z wykorzystaniem klasy 3 PoE (15.4W per 1 port).
3. Urządzenie musi obsługiwać minimum 4000 VLAN 802.1q
4. Urządzenie musi obsługiwać minimum 15000 adresów MAC

5. Urządzenie musi posiadać min. 2GB pamięci DRAM i 1GB pamięci flash
6. Parametry fizyczne – możliwość montażu w szafie 19", wielkość urządzenia nie może przekroczyć 1U
7. Minimalna wydajność przełączania ruchu 150Mpps (dla pakietów 64-bajtowych) oraz wymagana minimalna przepustowość matrycy 100Gb/s (200Gb/s full duplex)
8. Urządzenie musi posiadać funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:
   - Do min. 12 jednostek w stosie
   - Magistrala stakująca o przepustowości co najmniej 20Gbps (40Gbps Full Duplex)
   - Możliwość tworzenia połączeń EtherChannel LACP zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel) – minimum z 4 różnych przełączników w stosie jednocześnie
   - Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli itp. ich dostarczenie w ramach tego postępowania jest wymagane
9. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów (Jumbo Frames)
10. Urządzenie musi wspierać mechanizm QinQ
11. Zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)
12. Obsługa protokołu NTP lub SNTP
13. Musi zapewniać obsługę min. 12000 statycznych tras routingu IPv4.
14. Musi zapewniać routing statyczny oraz dynamiczny: OSPFv2, OSPFv3, RIP, RIP-NG.
15. Musi zapewniać obsługę protokołów First-Hop Redundancy - VRRP
16. Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping, PIM-SM, PIM-DM, PIM-SSM
17. Wsparcie dla protokołów Per-VLAN Spanning-Tree, IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 250 instancji protokołu STP
18. Wsparcie dla funkcji BPDU Guard oraz funkcji wykrywania i zabezpieczenia przed pętlami Layer 2.
19. Wsparcie dla funkcji Auto-MDI/MDI-X na portach 10/100/1000
20. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server oraz wspierać funkcję DHCP Helper
21. Funkcjonalność Layer 2 traceroute
22. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad.
23. Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:
   - Minimum 3 poziomów dostępu administracyjnego
   - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
   - Obsługa funkcji Guest VLAN
   - Obsługa Private VLAN
   - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
   - Możliwość uwierzytelniania użytkowników w oparciu o portal www (WebAuth)
   - Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC
   - Wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
   - Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
   - Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6
   - Obsługa list kontroli dostępu (ACL)
   - Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection
   - Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

- Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych, mechanizmy typu NetFlow lub równoważne - czyli umożliwienie zbierania pełnego lub próbkowanego ruchu sieciowego z określeniem źródła, przeznaczenia ruchu, klasy usługi, oraz przyczyn zatorów. Minimalne wymagane logowania jednego strumienia:
  i) Ingress interface (SNMP ifIndex)
  ii) Source IP address
  iii) Destination IP address
  iv) IP protocol
  v) Source port for UDP or TCP, 0 for other protocols
  vi) Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
  vii) IP Type of Service

24. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS)
    - Implementacja co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu WRR lub SRR lub innego podobnego dla obsługi tych kolejek
    - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    - Możliwość mapowania ruchu do określonych kolejek QoS z wykorzystaniem ACL
    - Możliwość ograniczania pasma dostępnego na każdym porcie jednocześnie dla ruchu wychodzącego oraz przychodzącego za pomocą Shapingu lub Policingu.
25. Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP) - protokół wykrywający sąsiednie urządzenia i ich atrybuty.
26. Obsługa protokołu UDLD lub Ethernet OAM.
27. Obsługa protokołu Ethernet Ring – Np. G.8032 lub REP lub inny równoważny - protokół pozwalający budować pierścienie zbudowane z kilku dostarczanych urządzeń, gdzie ruch przełącza się w czasach poniżej <1s bez wsparcia protokołu Spanning-Tree.
28. Obsługa protokołu GVRP lub MVRP lub innego równoważnego (np. VTP) - protokół dystrybuujący istniejące i wykorzystane sieci VLAN pomiędzy urządzeniami dostępowymi w sposób automatyczny (bez konieczności ręcznej konfiguracji przez administratora).
29. Obsługa protokołu OpenFlow 1.3 lub nowszego dla współpracy z kontrolerem OpenFlow.
30. Wsparcie dla AAA z wykorzystaniem serwerów Tacacs oraz Radius.
31. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli
32. Urządzenie musi posiadać port konsoli szeregowej oraz port Ethernet typu out-of-band – do zarządzania
33. Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash.
34. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego z wykorzystaniem funkcji ERSPAN
35. Musi być obsługiwana funkcja WriteNet - dzięki której przełącznik wykona upload swojego pliku konfiguracyjnego na zdalny serwer TFTP/SCP po otrzymaniu odpowiednich pakietów SNMP Write. Musi istnieć dodatkowe zabezpieczenie tej funkcji hasłem (np. enable) lub możliwość definiowana listy zaufanych serwerów TFTP/SCP.
36. Plik konfiguracyjny urządzenia musi być 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 nową konfiguracją.
37. MTBF (Mean Time Between Failure) dla każdego urządzenia tworzącego stos nie może być mniejszy niż 250000 godzin.

IV. Wymagania technicznie dla urządzeń typu Firewall.

Wymagania podstawowe

1. System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
2. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 5000 Mbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 2200 Mbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering), obsługiwać nie mniej niż 1000000 jednoczesnych połączeń oraz zapewniać wydajność nie mniejszą niż 2500 Mbit/s dla ruchu szyfrowanego IPSEC VPN.
3. System zabezpieczeń firewall musi być wyposażony w co najmniej:
    a. 12 portów Ethernet 1GbE RJ45
    b. 4 porty Ethernet 1GbE SFP
    c. 4 porty Ethernet 1/10GbE SFP/SFP+ (prędkość w 1Gb lub 10Gb w zależności od zainstalowanej wkładki)
    d. Porty SFP/SFP+ muszą współpracować z wkładkami innych producentów które posiada Zamawiający
4. System zabezpieczeń firewall musi być wyposażony w dwa redundantne zasilacze AC.
5. System zabezpieczeń firewall musi posiadać dołączony zestaw instalacyjny do szafy 19".
6. System zabezpieczeń firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując 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. Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
8. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
9. System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tablice routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF oraz wspierać balansowanie ECMP.
10. System zabezpieczeń firewall musi wspierać możliwość podzielenia urządzenia na logiczne/wirtualne instancje – osobne zarządzanie i monitoring każdej instancji, podział interfejsów fizycznych (porty Ethernet) oraz logicznych (tunele, loopback, sub-interfejsy VLAN) oraz reguł NAT/bezpieczeństwa pomiędzy instancjami. Urządzenie musi mieć możliwość rozbudowy do 5 logicznych/wirtualnych instancji. Jeśli funkcjonalność wymaga licencji nie jest konieczne jej dostarczenie na tym etapie postępowania.

11. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
12. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
13. System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
14. System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
15. 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. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 4900 Mbit/s.
16. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
17. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
18. Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
19. System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
20. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
21. System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
22. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
23. System zabezpieczeń firewall 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.

24. System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
25. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
26. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
27. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
28. System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
29. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

Wymagania podstawowe identyfikacji użytkowników

1. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) 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.
2. System zabezpieczeń firewall 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.
3. System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.

4. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day

1. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.
2. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
3. System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
4. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
5. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
6. System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
7. System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
8. System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
9. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
10. System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
11. System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

12. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
13. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
14. System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
15. System zabezpieczeń firewall 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.
16. System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
17. System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.
18. System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.

Wymagania dodatkowe: NAT, DoS, IPSEC VPN, SSL VPN, QoS

1. System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
2. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
3. System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
4. System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Należy zapewnić aby funkcja VPN (IPSec i SSL) umożliwiała obsługę min. 400 użytkowników. Jeżeli wymaga to zakupu dodatkowych licencji, należy uwzględnić odpowiednią ich ilość.
5. System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.
6. System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są

takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci. Jeśli funkcjonalność ta wymaga dodatkowych licencji – dostarczenie jej nie jest wymagane na tym etapie postępowania.

7. System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.
8. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
9. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
10. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

Wymagania dla zarządzania i raportowania

1. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
2. System zabezpieczeń firewall 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.
3. System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
4. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
5. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
6. 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.
7. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
8. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).

9. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 32 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
10. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
11. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
12. System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
13. System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
14. System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
15. System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
16. System zabezpieczeń firewall pozwalać na tworzenie wielu 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.
17. System zabezpieczeń firewall musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
18. System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

Wymagania dodatkowe - środowisko wirtualne VMware

1. System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.

Szkolenie certyfikowane

1. Zakres szkolenia: konfiguracja i administracja.
2. Ilość osób: 3
3. Termin szkolenia: do 90 dni roboczych od dnia podpisania protokołu odbioru.
4. Szkolenie musi być dostępne w Polsce oraz prowadzone w języku Polskim.

IV. Gwarancja

1. System musi być objęty minimum 36 miesięczną gwarancją autoryzowanego (certyfikowanego) centrum serwisowego w rygorze następny dzień roboczy. Obsługa zgłoszeń i kontakt serwisem musi być realizowany w języku Polskim. W ramach gwarancji muszą być serwisowane wszystkie elementy sprzętu, zapewniony dostęp do baz wiedzy producenta, aktualizacji oprogramowania oraz nieograniczony dostęp do TAC. W ramach gwarancji muszą być również dostępne wszystkie licencje/subskrypcje na okres minimum 36 miesięcy zapewniające opisane wyżej funkcjonalności.

Projekt współfinansowany jest przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju regionalnego w ramach Regionalnego Programu Operacyjnego – Lubuskie 2020,
Oś priorytetowa 2. "Rozwój Cyfrowy" Działanie 2.1 Rozwój społeczeństwa informacyjnego"