Załącznik nr 1 do zapytania

OPIS PRZEDMIOTU ZAMÓWIENIA

Rozbudowa sieci LAN

Termin realizacji zamówienia:

Do 50 dni roboczych.

Przedmiot zamówienia:

Zamówienie obejmuje:

a. Dostawę Urządzeń i oprogramowania opisanych szczegółowo w pkt 10.
b. Dostawa zostanie zrealizowana do siedziby firmy zlokalizowanej na terenie Warszawy.
c. Gwarancję na warunkach opisanych w pkt. 11.

Wymagania ogólne:

1. Wszystkie dostarczone Urządzenia zasilane prądem przemiennym muszą być zasilane napięciem 230 V/50 Hz.
2. Zamawiający wymaga, aby dostarczone Urządzenia były fabrycznie nowe (tzn. bez śladów używania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Rzeczpospolitej Polskiej.
3. Oferowane Urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
4. Wszystkie wymagane moduły SFP, SFP+, SFP28, QSFP muszą być producentów urządzeń.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

1. Przełącznik do styku z Internetem

Dostawa 4 urządzeń, każde o wymaganiach opisanych poniżej.

1.1. Przełącznik posiada:

a) 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+;

b) 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie100Gbps na pojedynczej parze okablowania multi-mode (do 100m).

1.2. Parametry wydajnościowe:

a) Prędkość przełączania 1.8Tbps full duplex;

b) Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.

1.3. Przełącznik posiada następującą funkcjonalność dla warstwy L2:

a) Trunking IEEE 802.1Q VLAN;

b) Wsparcie dla 3000 sieci VLAN;

c) Wsparcie sprzętowe dla 90 tysięcy adresów MAC;

d) IEEE 802.1w Rapid Spanning Tree (RST);

e) IEEE 802.1s Multiple Spanning Tree (MST);

f) Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU);

g) Internet Group Management Protocol (IGMP) wersje 2, 3;

h) Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach;

i) Link Aggregation Control Protocol (LACP): IEEE 802.3ad ;

j) Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);

k) Funkcjonalność izolowania portów znajdujących się w tym samym VLAN;

l) Wsparcie sprzętowe dla tunelowania QinQ i QinVNI.

1.4. Przełącznik posiada następującą funkcjonalność dla warstwy L3:

a) Sprzętowe przełączanie pakietów w warstwie L3;

b) Routing w oparciu o trasy statyczne;

c) Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6;

d) Policy Based Routing (PBR);

e) VRRP;

f) Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6;

g) Tunele GRE;

h) Wsparcie sprzętowe dla minimum 700 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP;

i) Wsparcie dla VRF;

j) Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP);

k) Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast);

l) Wsparcie dla IGMPv3 oraz MSDP;

m) Wsparcie sprzętowe dla minimum 32,000 tras multicastowych;

n) Obsługa minimum 4000 wpisów dla ACL (access control list).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

1.5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   a) Zintegrowany, sprzętowy VXLAN Bridging/Routing;
   b) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast);
   c) Implementacja VXLAN BGP EVPN (Ethernet VPN);
   d) Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).

1.6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   a) Layer 2 IEEE 802.1p (CoS) oraz DSCP;
   b) Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6);
   c) Kolejkowanie bezwzględne (strict-priority) ;
   d) Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection);
   e) Ograniczanie ruchu (policing) do żądanej przepływności;
   f) Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;
   g) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.

1.7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   a) Obsługa list kontroli dostępu (ACL);
      – ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
      – iACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
      – ACL oparte o porty (PACL).
   b) DHCP Snooping;
   c) ARP Inspection;
   d) IP Source Guard;
   e) Unicast reverse path forwarding (uRPF);
   f) Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.

1.8. Przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
   a) Port zarządzający 100/1000 Mbps;
   b) Port konsoli CLI;
   c) Zarządzanie In-band;
   d) SSHv2;
   e) Authentication, authorization and accounting (AAA);
   f) RADIUS;
   g) TACACS/TACACS+;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

h) Syslog;
i) SNMP v1, v2c, v3;
j) Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. co 30s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB;
k) Role-Based Access Control RBAC;
l) IEEE 802.1ab LLDP;
m) Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback);
n) 802.1x;
o) Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);
p) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring);
q) Network Time Protocol (NTP);
r) Precision Time Protocol IEEE 1588;
s) Diagnostyka procesu BOOT;
t) Ping;
u) Traceroute.

1.9. Narzędzia programowania i zarządzania przełącznikiem:
a) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API;
b) Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika;
c) Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika;
d) Interfejs programistyczny REST API wraz z upublicznionym SDK;
e) Wsparcie dla OpenStack Neutron plugin.

1.10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.

1.11. Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.

1.12. Wyposażenia przełącznika:
a) 16 wkładek 10G SFP+ SR,
b) 16 wkładek 1G SFP SX
c) 16 wkładek 1G RJ45.

2. Urządzenie typu router.

Dostawa 4 urządzeń, każde o wymaganiach opisanych poniżej.

2.1. Urządzenie o architekturze modularnej, wyposażone w 6 interfejsów Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP lub równoważnych, a także w 2 interfejsy

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

10 Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP+ lub równoważnych. Interfejsy 10GB muszą być aktywne, jeżeli wymaga to licencji to musi być ona dostarczona.

2.2. Urządzenie umożliwia rozszerzenie o co najmniej następujące typy interfejsów za pomocą modułów rozszerzeń:
   a) 1 port 10 GigabitEthernet;
   b) 8 portów Gigabit Ethernet;
   c) 4 interfejsy ATM STM1 lub 2 interfejsy STM4.

2.3. Urządzenie musi być dostarczone wraz z następującymi modułami SFP/SFP+:
   a) 4x moduł 10GB SR;
   b) 6x moduł 1GB SX;
   c) 6x moduł 1GB RJ45;

2.4. Urządzenie musi mieć możliwość instalacji przestrzeni dyskowej typu SSD o pojemności min. 100 GB.

2.5. Urządzenie posiada zasoby sprzętowe pozwalające przełączać 18 Mpps.

2.6. Urządzenie pozwala na przełączanie z prędkością 5 Gbps i umożliwia rozbudowę wydajności do co najmniej 20 Gbps bez modyfikacji sprzętowych.

2.7. Urządzenie posiada dedykowany akcelerator kryptograficzny osiągający wydajność co najmniej 10 Gbps dla ruchu IMIX.

2.8. Urządzenie posiada co najmniej 16 GB pamięci RAM.

2.9. Urządzenie obsługuje co najmniej 3 000 000 prefiksów w tablicach routing IPv4.

2.10. Urządzenie obsługuje co najmniej 3 000 000 prefiksów w tablicach routing IPv6.

2.11. Urządzenie obsługuje co najmniej 100 000 tras multicast.

2.12. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP.

2.13. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP.

2.14. Urządzenie obsługuje Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter) z możliwością definiowania polityk per aplikacja.

2.15. Urządzenie umożliwia uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routingu Forwarding), umożliwiając m.in. wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci.

2.16. Urządzenie obsługuje 8 000 instancji wirtualnych tablic routingu.

2.17. Urządzenie obsługuje funkcjonalność Bidirectional Forwarding Detection (BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego.

2.18. Urządzenie obsługuje funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF.

2.19. Urządzenie obsługuje multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN.

2.20. Urządzenie obsługuje protokół NHRP (ang. Next Hop Resolution Protocol).

2.21. Urządzenie obsługuje protokół GDOI (RFC 3547).

2.22. Funkcjonalności związane z niezawodnością pracy:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

a) redundancja procesów routingowych realizowana poprzez uruchomienie dwóch kopii systemu operacyjnego, jeżeli do otrzymania tej funkcjonalności jest wymagana licencja to nie jest wymagane dostarczenie jej;
b) BFD dla OSPF, BGP, ISIS;
c) IP FRR;
d) BGP Prefix-Independent Convergence (PIC);
e) Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP;
f) funkcjonalność VRRP;
g) redundantne zasilacze 230V;
h) możliwość wymiany modułów w trakcie pracy (ang. hot swap).

2.23. Urządzenie obsługuje MPLS, w szczególności:
a) LDP;
b) EoMPLS, VPLS;
c) MPLS L3 VPN;
d) MPLS TE;
e) MPLS FRR w trybach protekcji łącza oraz węzła.

2.24. Urządzenie obsługuje następujące mechanizmy jakości usług (QoS):
a) klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN zarówno dla IPv4 jak i IPv6;
b) hierarchiczny QoS (H-QoS) - co najmniej 3 poziomy;
c) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP;
d) dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek;
e) algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek;
f) możliwość obsługi jednej kolejki z priorytetem w stosunku do innych;
g) mechanizm ograniczania ilości ruchu w kolejce priorytetowej;
h) możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
i) możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting);
j) mechanizm WRED;
k) możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS.

2.25. Urządzenie obsługuje następujące funkcje i elementy bezpieczeństwa:
a) sprzętowa ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu;
b) Unicast RPF (Reverse Path Forwarding);
c) listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

d) 50 000 wpisów IPv4 na wszystkich listach kontroli dostępu (ACL), a także 4 000 list kontroli dostępu (ACL);
e) dostęp administracyjny oparty o role z przypisanymi uprawnieniami ;
f) zasoby sprzętowe umożliwiające uruchomienie funkcjonalności zapory ogniowej typu statefull (ang. statefull firewall), przy czym zapora ogniowa:
   - umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji),
   - obsługuje ruch IPv4 oraz IPv6,
   - umożliwia konfigurację polityk per wirtualna tablica routingu (VRF),
   - umożliwia obsługę 2 000 000 równoczesnych sesji,
   - umożliwia zestawianie 200 000 nowych połączeń HTTP na sekundę,
   - Jeżeli do otrzymania tej funkcjonalności jest wymagana licencja to nie jest wymagane dostarczenie jej.
g) zasoby sprzętowe realizujące funkcjonalności szyfrowania VPN z wydajnością 5 Gbps (AES256) z obsługą 8 000 tuneli IPSec;
h) sieci VPN typu site-2-site oparte o IPSec;
i) dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP w relacji spoke to spoke w celu optymalizacji transmisji danych pomiędzy oddziałami;
j) bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast;
k) algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), w szczególności:
   - Elliptic Curve Diffie-Hellman (ECDH),
   - Galois Counter Mode Advanced Encryption Standard (GCM-AES) - 128/256 bitów,
   - Galois Message Authentication Code (GMAC-AES) - 128/256 bitów,
   - Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2,
   - konfiguracja tuneli IPSec VPN w oparciu o protokół IKEv2,
   - IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych,
   - IKEv2 zarówno dla ruchu IPv4 jak i IPv6.
l) funkcjonalność VPN per VRF;
m) Jeżeli do otrzymania funkcjonalności VPN IPSec jest wymagana licencja to nie jest wymagane dostarczenie jej;
n) ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU;
o) logowanie pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU;
p) możliwość uruchomienia funkcjonalności analizy i klasyfikacji pakietów w warstwie 2-7 polegającej na przeszukiwaniu pakietów pod kątem zawierania specyficznych ciągów znaków i wykrywania na tej podstawie ataków.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

2.26. Urządzenie umożliwia uruchomienie usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów, przy czym klasyfikacja ta:
   a) opiera się na kilku mechanizmach gwarantujących poprawne rozpoznawanie wielu aplikacji / protokołów;
   b) udostępnia 3 atrybuty opisujące daną aplikację / protokół (atrybuty ułatwiają konfigurowanie QoS na urządzeniu poprzez grupowanie podobnych aplikacji / protokołów - na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji);
   c) nie wymaga rozbudowy sprzętowej urządzenia, jedynie zakup licencji .

2.27. Urządzenie obsługuje 4000 tuneli GRE.

2.28. Urządzenie posiada możliwość tunelowania przesyłanych danych w postaci tuneli GRE typu punkt-punkt oraz punkt-wielopunkt z możliwością uruchomienia protokołów routingu dynamicznego pomiędzy urządzeniami połączonymi za pomocą tuneli GRE.

2.29. Urządzenie umożliwia ochronę kryptograficzną tuneli GRE.

2.30. W ramach funkcjonalności zarządzania, urządzenie:
   a) umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3;
   b) obsługuje Ethernet OAM (IEEE 802.3ah, IEEE 802.1ag, ITU-T Y.1731);
   c) obsługuje MPLS OAM;
   d) umożliwia pisanie skryptów konfiguracyjnych;
   e) obsługuje protokół Netflow ze wsparciem dla multicast oraz IPv4/IPv6;
   f) posiada narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP;
   g) posiada obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+;
   h) posiada dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet 10/100/1000 oraz port AUX;
   i) posiada port USB;
   j) posiada możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej;
      – konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona
   k) urządzenie posiada możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów;

2.31. Urządzenie posiada redundantne zasilacze AC 230V zintegrowane w obudowie urządzenia.

2.32. Urządzenie umożliwia montaż w szafie 19”.

3. Przełącznik typu Leaf 1/10/25GE typ 1

Dostawa 2 urządzeń, każde o wymaganiach opisanych poniżej.

3.1 Przełącznik posiada:
   a) 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

b) 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie100Gbps na pojedynczej parze okablowania multi-mode (do 100m).

3.2 Parametry wydajnościowe:

a) Prędkość przełączania 1.8Tbps full duplex;

b) Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.

3.3 Przełącznik posiada następującą funkcjonalność dla warstwy L2:

a) Trunking IEEE 802.1Q VLAN;

b) Wsparcie dla 3000 sieci VLAN;

c) Wsparcie sprzętowe dla 90 tysięcy adresów MAC;

d) IEEE 802.1w Rapid Spanning Tree (RST);

e) IEEE 802.1s Multiple Spanning Tree (MST);

f) Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU);

g) Internet Group Management Protocol (IGMP) wersje 2, 3;

h) Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach;

i) Link Aggregation Control Protocol (LACP): IEEE 802.3ad ;

j) Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);

k) Funkcjonalność izolowania portów znajdujących się w tym samym VLAN;

l) Wsparcie sprzętowe dla tunelowania QinQ i QinVNI.

3.4 Przełącznik posiada następującą funkcjonalność dla warstwy L3:

a) Sprzętowe przełączanie pakietów w warstwie L3;

b) Routing w oparciu o trasy statyczne;

c) Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6;

d) Policy Based Routing (PBR);

e) VRRP;

f) Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6;

g) Tunele GRE;

h) Wsparcie sprzętowe dla minimum 700 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP;

i) Wsparcie dla VRF;

j) Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP);

k) Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast);

l) Wsparcie dla IGMPv3 oraz MSDP;

m) Wsparcie sprzętowe dla minimum 32,000 tras multicastowych;

n) Obsługa minimum 4000 wpisów dla ACL (access control list).

3.5 Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:

a) Zintegrowany, sprzętowy VXLAN Bridging/Routing;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

b) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast);
c) Implementacja VXLAN BGP EVPN (Ethernet VPN);
d) Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).

3.6 Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
a) Layer 2 IEEE 802.1p (CoS) oraz DSCP;
b) Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6);
c) Kolejkowanie bezwzględne (strict-priority) ;
d) Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection);
e) Ograniczanie ruchu (policing) do żądanej przepływności;
f) Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;
g) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.

3.7 Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
a) Obsługa list kontroli dostępu (ACL);
– ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
– iACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
– ACL oparte o porty (PACL).
b) DHCP Snooping;
c) ARP Inspection;
d) IP Source Guard;
e) Unicast reverse path forwarding (uRPF);
f) Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast,
multicast, broadcast.

3.8 Przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia
przełącznika:
a) Port zarządzający 100/1000 Mbps;
b) Port konsoli CLI;
c) Zarządzanie In-band;
d) SSHv2;
e) Authentication, authorization and accounting (AAA);
f) RADIUS;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

g) TACACS/TACACS+;
h) Syslog;
i) SNMP v1, v2c, v3;
j) Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. co 30s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB;
k) Role-Based Access Control RBAC;
l) IEEE 802.1ab LLDP;
m) Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback);
n) 802.1x;
o) Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);
p) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring);
q) Network Time Protocol (NTP);
r) Precision Time Protocol IEEE 1588;
s) Diagnostyka procesu BOOT;
t) Ping;
u) Traceroute.

3.9 Narzędzia programowania i zarządzania przełącznikiem:
a) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku
i konfiguracji przełącznika poprzez API;
b) Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika;
c) Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika;
d) Interfejs programistyczny REST API wraz z upublicznionym SDK;
e) Wsparcie dla OpenStack Neutron plugin.

3.10 Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.

3.11 Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.

3.12 Wyposażenia przełącznika:
a) 2 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional);
b) 30 wkładek 25G SFP+ SR;
c) 20 wkładek 1G SFP RJ45;
d) 30 wkładek 10G SFP+ SR;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

3.13 Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem zarządzającym CISCO ACI SDN. Istnieje możliwość zmiany trybu pracy (np. poprzez wymianę oprogramowania lub wgranie odpowiedniej licencji jeśli potrzebne), nie dopuszcza się konieczności modyfikacji sprzętowej urządzeń. Jeśli dla celów realizacji tych funkcjonalności konieczna jest dla przełącznika licencja to wymaga się jej dostarczenia. Jeśli licencja jest realizowana w modelu subskrypcyjnym wymaga się dostarczenia jej na min 36 miesięcy.

4. Zapora ogniowa typ 1

Dostawa 2 urządzeń, każde o wymaganiach opisanych poniżej

4.1 W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
4.2 W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
4.3 Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4.4 Monitoring stanu realizowanych połączeń VPN.
4.5 System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
4.6 System realizujący funkcję Firewall musi dysponować minimum:
4.7 10 portami Gigabit Ethernet RJ-45.
4.8 8 gniazdami SFP 1 Gbps.
4.9 2 gniazdami SFP+ 10 Gbps.
4.10 System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
4.11 W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4.12 System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.
4.13 System musi być wyposażony w zasilanie AC.
4.14 W zakresie Firewall'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 450 tys. nowych połączeń na sekundę.
4.15 Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 512 B.
4.16 Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 15 Gbps.
4.17 Wydajność szyfrowania IPSec VPN nie mniej niż 20 Gbps.
4.18 Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 10 Gbps.
4.19 Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.
4.20 Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8 Gbps.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.21 W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
   a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
   b) Kontrola Aplikacji.
   c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
   d) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
   e) Ochrona przed atakami - Intrusion Prevention System.
   f) Kontrola stron WWW.
   g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
   h) Zarządzanie pasmem (QoS, Traffic shaping).

4.22 Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

4.23 Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

4.24 Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

4.25 Analiza ruchu szyfrowanego protokołem SSH.

4.26 Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

4.27 Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

4.28 System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   a) Translację jeden do jeden oraz jeden do wielu.
   b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

4.29 W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4.30 Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

4.31 Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   a) Amazon Web Services (AWS).
   b) Microsoft Azure
   c) Google Cloud Platform (GCP).
   d) OpenStack.
   e) VMware NSX.

4.32 System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   a) Wsparcie dla IKE v1 oraz v2.
   b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

c) Obsługa protokołu Diffie-Hellman grup 19 i 20.
d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
i) Mechanizm „Split tunneling" dla połączeń Client-to-Site.

4.33 System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

4.34 W zakresie routingu rozwiązanie powinno zapewniać obsługę:
a) Routingu statycznego.
b) Policy Based Routingu.
c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

4.35 System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

4.36 Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

4.37 System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

4.38 Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

4.39 System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

4.40 Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

4.41 System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

4.42 System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

4.43 System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

4.44 System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

4.45 Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.46 Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

4.47 System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

4.48 Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4.49 Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

4.50 System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

4.51 Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

4.52 Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

4.53 Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

4.54 Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4.55 Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4.56 Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

4.57 Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

4.58 Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

4.59 W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

4.60 Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4.61 Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

4.62 Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

4.63 Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

4.64 W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

4.65 System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.66 Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

4.67 Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

4.68 Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

4.69 Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

4.70 Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

4.71 Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4.72 System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

4.73 System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

4.74 Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

4.75 Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

4.76 Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

4.77 W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

4.78 Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4.79 Musi istnieć możliwość logowania do serwera SYSLOG.

4.80 Wyposażenie dodatkowe na urządzenie:

a) 2 wkładki 10G SFP+ SR
b) 8 wkładek 1G SFP SR

4.81 Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

a) ICSA lub EAL4 dla funkcji Firewall.

4.82 W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

5. Zapora ogniowa typ 2

Dostawa 2 urządzeń, każde o wymaganiach opisanych poniżej

5.1 W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

5.2 W ramach postępowania system musi zostać dostarczony w postaci redundantnej.

5.3 Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

5.4 Monitoring stanu realizowanych połączeń VPN.

5.5 System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

5.6 System realizujący funkcję Firewall musi dysponować minimum:

a) 16 portami Gigabit Ethernet RJ-45.
b) 8 gniazdami SFP 1 Gbps.
c) 8 gniazdami SFP+ 10 Gbps.
d) 2 gniazdami QSFP+ 40 Gbps.

5.7 System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

5.8 W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

5.9 System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 960 GB.

5.10 System musi być wyposażony w zasilanie 2xAC.

5.11 W zakresie Firewall'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 480 tyś. nowych połączeń na sekundę.

5.12 Przepustowość Stateful Firewall: nie mniej niż 80 Gbps dla pakietów 512 B.

5.13 Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 25 Gbps.

5.14 Wydajność szyfrowania IPSec VPN nie mniej niż 46 Gbps.

5.15 Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 12 Gbps.

5.16 Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.

5.17 Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 10 Gbps.

5.18 W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

b) Kontrola Aplikacji.
c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
d) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
e) Ochrona przed atakami - Intrusion Prevention System.
f) Kontrola stron WWW.
g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
h) Zarządzanie pasmem (QoS, Traffic shaping).
i) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

5.19 Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

5.20 Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.

5.21 Analiza ruchu szyfrowanego protokołem SSH.

5.22 Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

5.23 Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

5.24 System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

a) Translację jeden do jeden oraz jeden do wielu.
b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

5.25 W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

5.26 Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.

5.27 Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

a) Amazon Web Services (AWS).
b) Microsoft Azure
c) Google Cloud Platform (GCP).
d) OpenStack.
e) VMware NSX.

5.28 System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

5.29 Wsparcie dla IKE v1 oraz v2.

5.30 Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

5.31 Obsługa protokołu Diffie-Hellman grup 19 i 20.

5.32 Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

5.33 Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5.34 Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
5.35 Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
5.36 Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
5.37 Mechanizm „Split tunneling" dla połączeń Client-to-Site.
5.38 System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
    b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
5.39 Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
5.40 W zakresie routingu rozwiązanie powinno zapewniać obsługę:
5.41 Routingu statycznego.
5.42 Policy Based Routingu.
5.43 Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
5.44 System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
5.45 Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
5.46 System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
5.47 Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
5.48 System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
5.49 Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
5.50 System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
5.51 System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
5.52 System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5.53 System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
5.54 Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
5.55 Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
5.56 System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
5.57 Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
5.58 Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5.59 System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5.60 Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
5.61 Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
5.62 Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
5.63 Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
5.64 Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
5.65 Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5.66 Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
5.67 Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
5.68 W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
5.69 Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
5.70 Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5.71 Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
5.72 Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
5.73 W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
5.74 System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
5.77 Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
5.78 Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
5.79 Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
5.80 Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5.81 Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
5.82 Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
5.83 System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5.84 System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
5.85 Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
5.86 Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
5.87 Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
5.88 W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
5.89 Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
5.90 Wyposażenie dodatkowe na urządzenia:
a) 8 wkładek 1G SFP SR
b) 8 wkładek 10G SFP+ SR
c) 2 wkładek 40G QFSP SR
5.91 Musi istnieć możliwość logowania do serwera SYSLOG. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:
a) ICSA lub EAL4 dla funkcji Firewall.
5.91 W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

6. Przełącznik typu Leaf 1/10/25GE typ 2

Dostawa 12 urządzeń, każde o wymaganiach opisanych poniżej.

6.1. Przełącznik posiada:
a) 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

b) 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie100Gbps na pojedynczej parze okablowania multi-mode (do 100m).

6.2. Parametry wydajnościowe:
   a) Prędkość przełączania 1.8Tbps full duplex;
   b) Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.

6.3. Przełącznik posiada następującą funkcjonalność dla warstwy L2:
   a) Trunking IEEE 802.1Q VLAN;
   b) Wsparcie dla 3000 sieci VLAN;
   c) Wsparcie sprzętowe dla 90 tysięcy adresów MAC;
   d) IEEE 802.1w Rapid Spanning Tree (RST);
   e) IEEE 802.1s Multiple Spanning Tree (MST);
   f) Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU);
   g) Internet Group Management Protocol (IGMP) wersje 2, 3;
   h) Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach;
   i) Link Aggregation Control Protocol (LACP): IEEE 802.3ad ;
   j) Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
   k) Funkcjonalność izolowania portów znajdujących się w tym samym VLAN;
   l) Wsparcie sprzętowe dla tunelowania QinQ i QinVNI.

6.4. Przełącznik posiada następującą funkcjonalność dla warstwy L3:
   a) Sprzętowe przełączanie pakietów w warstwie L3;
   b) Routing w oparciu o trasy statyczne;
   c) Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6;
   d) Policy Based Routing (PBR);
   e) VRRP;
   f) Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6;
   g) Tunele GRE;
   h) Wsparcie sprzętowe dla minimum 700 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP;
   i) Wsparcie dla VRF;
   j) Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP);
   k) Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast);
   l) Wsparcie dla IGMPv3 oraz MSDP;
   m) Wsparcie sprzętowe dla minimum 32,000 tras multicastowych;
   n) Obsługa minimum 4000 wpisów dla ACL (access control list).

6.5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   a) Zintegrowany, sprzętowy VXLAN Bridging/Routing;
   b) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast);

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

c) Implementacja VXLAN BGP EVPN (Ethernet VPN);
d) Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).

6.6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
a) Layer 2 IEEE 802.1p (CoS) oraz DSCP;
b) Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6);
c) Kolejkowanie bezwzględne (strict-priority) ;
d) Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection);
e) Ograniczanie ruchu (policing) do żądanej przepływności;
f) Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;
g) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.

6.7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
a) Obsługa list kontroli dostępu (ACL);
– ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
– iACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
– ACL oparte o porty (PACL).
b) DHCP Snooping;
c) ARP Inspection;
d) IP Source Guard;
e) Unicast reverse path forwarding (uRPF);
f) Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.

6.8. Przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
a) Port zarządzający 100/1000 Mbps;
b) Port konsoli CLI;
c) Zarządzanie In-band;
d) SSHv2;
e) Authentication, authorization and accounting (AAA);
f) RADIUS;
g) TACACS/TACACS+;
h) Syslog;
i) SNMP v1, v2c, v3;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

j) Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. co 30s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB;
k) Role-Based Access Control RBAC;
l) IEEE 802.1ab LLDP;
m) Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback);
n) 802.1x;
o) Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);
p) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring);
q) Network Time Protocol (NTP);
r) Precision Time Protocol IEEE 1588;
s) Diagnostyka procesu BOOT;
t) Ping;
u) Traceroute.

6.9. Narzędzia programowania i zarządzania przełącznikiem:
a) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API;
b) Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika;
c) Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika;
d) Interfejs programistyczny REST API wraz z upublicznionym SDK;
e) Wsparcie dla OpenStack Neutron plugin.

6.10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.

6.11. Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.

6.12. Wyposażenia przełącznika:
a) 4 wkładki QSFP 100GE umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional);
b) 32 wkładki 10/25G SFP+ CSR.

6.13. Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem zarządzającym (kontrolerem SDN dostarczonym w ramach postępowania). Istnieje możliwość zmiany trybu pracy (np. poprzez wymianę oprogramowania lub wgranie odpowiedniej licencji jeśli potrzebne), nie dopuszcza się konieczności modyfikacji sprzętowej urządzeń. Jeśli dla celów realizacji tych funkcjonalności konieczna jest dla przełącznika licencja to wymaga się jej dostarczenia. Jeśli licencja jest realizowana w modelu subskrypcyjnym wymaga się dostarczenia jej na min 36 miesięcy. Zamawiający posiada system SDN CISCO ACI, którego funkcjonalności opisane zostały w pkt. 12 poniżej. Dostarczone przełączniki muszą w pełni współpracować z posiadanym systemem i jego funkcjonalnościami i być wyposażone w niezbędne w tym celu licencje.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

7. Przełącznik MGMT typ 1

Dostawa 4 urządzeń, każde o wymaganiach opisanych poniżej.

7.1. Przełącznik posiada:

c) 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+;

d) 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie100Gbps na pojedynczej parze okablowania multi-mode (do 100m).

7.2. Parametry wydajnościowe:

c) Prędkość przełączania 1.8Tbps full duplex;

d) Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.

7.3. Przełącznik posiada następującą funkcjonalność dla warstwy L2:

m) Trunking IEEE 802.1Q VLAN;

n) Wsparcie dla 3000 sieci VLAN;

o) Wsparcie sprzętowe dla 90 tysięcy adresów MAC;

p) IEEE 802.1w Rapid Spanning Tree (RST);

q) IEEE 802.1s Multiple Spanning Tree (MST);

r) Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU);

s) Internet Group Management Protocol (IGMP) wersje 2, 3;

t) Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach;

u) Link Aggregation Control Protocol (LACP): IEEE 802.3ad ;

v) Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);

w) Funkcjonalność izolowania portów znajdujących się w tym samym VLAN;

x) Wsparcie sprzętowe dla tunelowania QinQ i QinVNI.

7.4. Przełącznik posiada następującą funkcjonalność dla warstwy L3:

o) Sprzętowe przełączanie pakietów w warstwie L3;

p) Routing w oparciu o trasy statyczne;

q) Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6;

r) Policy Based Routing (PBR);

s) VRRP;

t) Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6;

u) Tunele GRE;

v) Wsparcie sprzętowe dla minimum 700 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP;

w) Wsparcie dla VRF;

x) Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP);

y) Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast);

z) Wsparcie dla IGMPv3 oraz MSDP;

aa) Wsparcie sprzętowe dla minimum 32,000 tras multicastowych;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

bb) Obsługa minimum 4000 wpisów dla ACL (access control list).

7.5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   e) Zintegrowany, sprzętowy VXLAN Bridging/Routing;
   f) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast);
   g) Implementacja VXLAN BGP EVPN (Ethernet VPN);
   h) Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).

7.6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   h) Layer 2 IEEE 802.1p (CoS) oraz DSCP;
   i) Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6);
   j) Kolejkowanie bezwzględne (strict-priority) ;
   k) Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection);
   l) Ograniczanie ruchu (policing) do żądanej przepływności;
   m) Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;
   n) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.

7.7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   g) Obsługa list kontroli dostępu (ACL);
      – ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
      – iACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
      – ACL oparte o porty (PACL).
   h) DHCP Snooping;
   i) ARP Inspection;
   j) IP Source Guard;
   k) Unicast reverse path forwarding (uRPF);
   l) Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.

7.8. Przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
   v) Port zarządzający 100/1000 Mbps;
   w) Port konsoli CLI;
   x) Zarządzanie In-band;
   y) SSHv2;
   z) Authentication, authorization and accounting (AAA);
   aa) RADIUS;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

bb) TACACS/TACACS+;
cc) Syslog;
dd) SNMP v1, v2c, v3;
ee) Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. co 30s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB;
ff) Role-Based Access Control RBAC;
gg) IEEE 802.1ab LLDP;
hh) Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback);
ii) 802.1x;
jj) Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);
kk) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring);
ll) Network Time Protocol (NTP);
mm) Precision Time Protocol IEEE 1588;
nn) Diagnostyka procesu BOOT;
oo) Ping;
pp) Traceroute.

7.9. Narzędzia programowania i zarządzania przełącznikiem:
f) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API;
g) Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika;
h) Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika;
i) Interfejs programistyczny REST API wraz z upublicznionym SDK;
j) Wsparcie dla OpenStack Neutron plugin.

7.10. Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.

7.11. Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.

7.12. Wyposażenia przełącznika:
a) 16 wkładek 10/25G SFP+ CSR,
b) 24 wkładki 1G RJ45.
c) Kabel 100GBASE-CR4 Passive Copper Cable, 1m

8. Przełącznik typu MGMT typ 2

Dostawa 2 urządzeń, każde o wymaganiach opisanych poniżej.

8.1. Przełącznik posiada:
a) 48 portów 100Mb/1GBaseT;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

b) 4 porty SFP+ 1/10/25 Gbpsb;
c) 2 porty definiowane za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps.

8.2. Parametry wydajnościowe:
a) Prędkość przełączania „wirespeed" dla każdego portu przełącznika;
b) Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3;
c) Obsługiwana łączna przepływność (pasmo) min. 600 Gbps;
d) Obsługiwana łączna przepustowość pakietowa przełącznika min. 250 mpps;
e) opóźnienie przełączania pakietów nie większe niż 3 µs;
f) głębokość buforów min. 40 MB;
g) pamięć RAM min. 24 GB;
h) Pamięć SSD/FLASH 128GB.

8.3. Przełącznik posiada następującą funkcjonalność warstwy L2:
a) Trunking IEEE 802.1Q VLAN;
b) Wsparcie dla 3900 sieci VLAN;
c) Funkcjonalność izolowania portów znajdujących się w tym samym VLAN;
d) Wsparcie sprzętowe dla minimum 90 tysięcy adresów MAC;
e) IEEE 802.1w Rapid Spanning Tree (RST);
f) IEEE 802.1s Multiple Spanning Tree (MST);
g) Wsparcie sprzętowe dla tunelowania QinQ;
h) Zabezpieczenie przeciwko incydentom w topologii Spanning Tree;
i) Internet Group Management Protocol (IGMP) Versions 2, 3;
j) Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach ;
k) Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązce;
l) Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów).

8.4. Przełącznik posiada następująca funkcjonalność warstwy L3
a) Sprzętowe przełączanie pakietów w warstwie L3;
b) Routing w oparciu o trasy statyczne;
c) Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6;
d) Policy Based Routing (PBR) dla IPv4;
e) VRRP v3;
f) Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol);
g) Wsparcie sprzętowe dla minimum 700 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP;
h) Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast);
i) Wsparcie dla IGMPv3 oraz MSDP;
j) Wsparcie sprzętowe dla minimum 32,000 tras multicastowych;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

k) Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking);
l) Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP);
m) Minimum 2000 wpisów dla ACL - access control list;
n) Jeśli funkcjonalność powyższa wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie.

8.5. Przełącznik posiada sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad i z wykorzystaniem klucza 256 bit. Jeśli funkcjonalność ta wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie.

8.6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
a) Layer 2 IEEE 802.1p (CoS);
b) Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4;
c) Kolejkowanie na wyjściu w oparciu o CoS 802.1p;
d) Bezwzględne (strict-priority) kolejkowanie na wyjściu;
e) Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający
f) Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych;
g) Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych;
h) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb;

8.7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
a) Wejściowe ACL (standardowe oraz rozszerzone);
- Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
- Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
- ACL oparte o VLAN-y (VACL);
- ACL oparte o porty (PACL);

b) DHCP Snooping;
c) ARP Inspection;
d) IP Source Guard;
e) Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.

8.8. Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
a) Port zarządzający 100/1000 Mbps;
b) Port konsoli CLI;
c) Zarządzanie In-band;
d) SSHv2;
e) Authentication, authorization, and accounting (AAA);
f) RADIUS;
g) TACACS+

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

h) Syslog;
i) SNMP v1, v2, v3;
j) RMON (przynajmniej grupy Events, Alarms);
k) sFlow lub netFlow;
l) IEEE 802.1ab LLDP;
m) Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
n) Role-Based Access Control RBAC;
o) Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);
p) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror);
q) Network Time Protocol (NTP);
r) Precision Time Protocol IEEE 1588;
s) Diagnostyka procesu BOOT;
t) Ping;
u) Traceroute.

8.9. Narzędzia programowania i zarzadzania przełącznikiem:
a) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API;
b) Wbudowana powłoka bash do zarządzania systemem Linux przełącznika;
c) Wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. Kontener posiada możliwość wykorzystywania portów fizycznych przełącznika;
d) Interfejs programistyczny REST API wraz z upublicznionym SDK;
e) Wsparcie dla NETCONF i zarządzania poprzez XML;
f) Wsparcie dla OpenStack Neutron plugin.

8.10. Przełącznik musi być wyposażony w:
a) 2 wkładki QSFP 100GE umozliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional).

8.11. Przełącznik musi być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych lub połączeń zasilających urządzenia.

8.12. Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.

8.13. Wyposażenia przełącznika:
a) 4 wkładki 10/25G SFP+ CSR.

9. Konsola terminali

Dostawa 4 urządzeń, każde o wymaganiach opisanych poniżej.

9.1. Urządzenie typu modularnego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

9.2. Urządzenie musi pozwalać na instalację co najmniej:
   a) 4 kart sieciowych z interfejsami,
   b) 1 modułu usługowego z interfejsami. Moduły usługowe muszą mieć możliwość wyłączenia w celu oszczędzania energii elektrycznej,
   c) 1 wewnętrznego modułu usługowego.

9.3. Musi posiadać zainstalowany wewnętrzny sprzętowy moduł akceleracji szyfrowania DES/3DES/AES ze wsparciem standardu Suite-B.

9.4. Musi posiadać możliwość skonfigurowania bezpośredniej komunikacji pomiędzy wybranymi modułami usługowymi z pominięciem głównego procesora.

9.5. Musi posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.

9.6. Urządzenie musi oferować dla pakietów o długości 64bajtów wydajność co najmniej 353 kps/180Mbps.

9.7. Musi posiadać obsługę routingu statycznego.

9.8. Musi posiadać wsparcie dla funkcjonalności Policy Based Routing.

9.9. Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF).

9.10. Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q.

9.11. Musi obsługiwać IPv6 w tym ICMP dla IPv6.

9.12. Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL.

9.13. Musi obsługiwać protokół NTP.

9.14. Musi obsługiwać DHCP w zakresie Client , Server.

9.15. Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika).

9.16. Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+.

9.17. Musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (tzw. Embedded Event Monitor – EEM, lub odpowiednik).

9.18. Funkcjonalność EEM musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych.

9.19. Funkcjonalność EEM musi pozwalać na generowanie akcji:
   a) Wykonanie komendy z poziomu linii poleceń urządzenia,
   b) Wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej,
   c) Wykonanie skryptu,
   d) Wygenerowanie SNMP trap,
   e) Ustawienie lub modyfikacja określonego licznika systemowego.

9.20. Musi być zarządzane za pomocą protokołów SNMPv1, SNMPv2, SNMPv3, SSH.

9.21. Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Neftflow/JFlow lub odpowiednika.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

9.22. Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI).

9.23. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

9.24. Możliwość montażu urządzenia w szafie 19”.

9.25. Urządzenie musi mieć możliwość zasilania ze źródeł zmiennoprądowych 230V (zasilacze AC) oraz stałoprądowych (zasilacze DC - funkcja wymagana ale nie wymaga się na etapie zamówienia dostarczenia tego typu zasilania).

9.26. Wyposażenia urządzenia:

a) 3 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci LAN,
b) 32 porty asynchroniczne wraz z odpowiednim okablowaniem,
c) Wszystkie karty i moduły muszą być objęte wspólnym serwisem producenta.

10. System uwierzytelnienia i monitorowania administratorów urządzeń sieciowych

10.1. Podstawowe cechy systemu

10.1.1. System musi składać się z dwóch urządzeń fizycznych lub maszyn wirtualnych tworzący klaster HA.

10.1.2. System umożliwia instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym:

a) VMWare vSphere w wersji 6.7 i wyższych
b) KVM na Red Hat Enterprise Linux (RHEL) 7.0
c) Microsoft Hyper-V
d) na serwerach fizycznych wspieranych przez producenta

10.1.3. System umożliwia konfigurację za pomocą interfejsu graficznego (GUI) z wykorzystaniem przeglądarki web.

10.1.4. System umożliwia aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS.

10.1.5. System umożliwia zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).

10.1.6. System umożliwia tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).

10.1.7. System umożliwia uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.

10.1.8. System umożliwia wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System wymusza hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni

10.1.9. System umożliwia kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

a) dostęp do interfejsu konfiguracji urządzeń sieciowych
b) dostęp do interfejsu konfiguracji polityk
c) dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
d) System umożliwia kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.

10.2. Mechanizmy uwierzytelniania

10.2.1. System wspiera następujące protokoły uwierzytelniania i standardy:
a) RADIUS, zgodnie z dokumentami:
- RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
- RFC 2139 — RADIUS Accounting
- RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 — RADIUS Accounting
- RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
- RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 — RADIUS Extensions

b) Obsługa protokołu TACACS+ do administracji urządzeniami sieciowymi

10.2.2. System wspiera protokół Windows Active Directory, w tym następujące repozytoria AD:
a) Microsoft Windows Active Directory 2003 32bit
b) Microsoft Windows Active Directory 2003 R2 32bit i 64bit
c) Microsoft Windows Active Directory 2008 32bit i 64bit
d) Microsoft Windows Active Directory 2008 R2 64bit
e) Microsoft Windows Active Directory 2012
f) Microsoft Windows Active Directory 2012 R2
g) Microsoft Windows Active Directory 2016

10.2.3. System wspiera protokół Lightweight Directory Access Protocol (LDAP)

10.2.4. System wspiera serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865

10.2.5. System wspiera następujące protokoły uwierzytelniania:
a) PAP/ASCII
b) CHAP
c) MS-CHAPv1
d) MS-CHAPv2
e) EAP-MD5
f) LEAP
g) EAP-TLS
h) Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
- EAP-MS-CHAPv2
- EAP-GTC
- EAP-TLS

i) System umożliwia konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

10.2.6. System posiada lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)

10.3. Raportowanie. System umożliwiać generowanie m.in. następujących raportów:

10.3.1. raportów dla protokołów AAA:
- a) diagnostyki protokołów AAA
- b) accountingu RADIUS
- c) uwierzytelniania RADIUS
- d) accountingu TACACS
- e) uwierzytelniania TACACS

10.3.2. raportów dozwolonych protokołów
- a) sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:
  - uwierzytelnień pomyślnych
  - uwierzytelnień nieudanych
- b) „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:
  - uwierzytelnień pomyślnych
  - uwierzytelnień nieudanych

10.3.3. raportów dla poszczególnych instancji serwerów systemu, w tym:
- a) uwierzytelnień RADIUS per serwer
- b) Top „N" uwierzytelnień per serwer
- c) monitorowania Online Certificate Status Protocol (OCSP)
- d) administratorów systemu i ich uprawnień
- e) logowania administratorów do systemu
- f) zmian konfiguracji serwera dokonanych przez administratorów
- g) stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
- h) zmian operacyjnych serwera dokonanych przez administratorów
- i) zmian haseł przez użytkowników

10.3.4. raportów dla błędów, w tym:
- a) błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
- b) sumarycznych przyczyn nieudanych uwierzytelnień
- c) Top „N" uwierzytelnień per rodzaj błędu

10.3.5. raportów dla urządzeń sieciowych:
- a) sumarycznych uwierzytelnień dla urządzeń sieciowych
- b) Top „N" uwierzytelnień per urządzenie sieciowe
- c) niedostępności serwera AAA dla urządzenia sieciowego
- d) wiadomości logowanych przez urządzenia sieciowe
- e) stanu portów i sesji urządzenia sieciowego widocznych przez SNMP

10.3.6. raportów użytkowników:
- a) sumarycznych uwierzytelnień użytkowników
- b) Top „N" uwierzytelnień per użytkownik
- c) uwierzytelnień per unikalny użytkownik

10.3.7. raportów katalogu sesji
- a) aktywnych sesji RADIUS
- b) historii sesji RADIUS

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

c) zaterminowanych sesji RADIUS

10.4. Alarmy

10.4.1. System umożliwia generowanie alarmów systemowych w sytuacjach krytycznych za pomocą
   a) wiadomości e-mail
   b) syslog

10.4.2. Alarmy mogą być generowane w następujących sytuacjach:
   a) ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu
   b) opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego
   c) status krytycznych procesów będzie niepożądany, w tym status:
      - procesu wewnętrznej bazy danych systemu
      - serwera aplikacyjnego systemu
      - bazy danych sesji
      - kolektora i procesora wiadomości log
      - błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej)
      - stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:
        - obciążenie systemu (load)
        - zajętość pamięci

10.4.3. System posiada zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
   a) badanie łączności IP za pomocą ping, nslookup, traceroute
   b) wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
      - nazwy użytkownika
      - statusu uwierzytelnienia (udana lub nieudana)
      - powodu, jeżeli uwierzytelnienie nieudane
      - zakresu czasowego, co do dnia, godziny i minuty
   c) wykonanie zdalnego polecenia na urządzeniu sieciowym
   d) ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
      - definicji serwerów AAA
      - protokołu RADIUS
      - odkrywania urządzeń
      - logowania
   e) wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu

11. Gwarancja

11.1. Dostawca gwarantuje, że każdy produkt, który zostanie dostarczony jest fabrycznie nowy i pochodzi bezpośrednio od producenta lub autoryzowanego sprzedawcy.

11.2. Urządzenia muszą być objęte przynajmniej 36 miesięczną gwarancją od dnia podpisania Protokołu Odbioru wnioskującego o rozliczenie finansowe. Zamawiający dopuszcza świadczenie gwarancji bezpośrednio przez producenta lub partnera producenta przy

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

wsparciu producenta w reżimie 8x5xNBD (tj. 8 godzin w dni robocze) uprawniającym do wsparcia telefonicznego i mailowego w zakresie konfiguracji Urządzenia oraz dającym prawo do aktualizacji oprogramowania, a w przypadku ujawnienia wad w okresie gwarancji Wykonawca w ramach gwarancji zobowiązuje się w terminie nie dłuższym niż 5 dni roboczych od dnia zgłoszenia tego faktu przez Zamawiającego (reklamacja) do:

a) usunięcia wad Urządzenia w siedzibie Zamawiającego lub, jeżeli usunięcie wady w siedzibie nie jest możliwe, usunięcia wady poza siedzibą Zamawiającego. W przypadku, gdy Wykonawca wykonuje naprawę poza siedzibą Zamawiającego, jest on zobowiązany na czas naprawy udostępnić Zamawiającemu i dostarczyć na własny koszt sprzęt zastępczy o parametrach nie gorszych od Urządzenia naprawianego. Koszty związane z dostarczeniem urządzenia zastępczego ponosi Wykonawca;
b) wymiany Urządzenia na nowe, wolne od wad.

12. System Software Defined Networking (SDN) posiadany przez Zamawiającego

12.1. Rozwiązanie składa się z uzupełniających się komponentów sprzętowych i programowych tworzących wspólną całość:

a) Centralnego kontrolera SDN zarządzającego siecią fizyczną, wirtualną, kontenerową oraz warstwą logiczną i zapewniającego uruchamianie usług w oparciu o modelowanie polityk dla aplikacji,
b) Infrastruktury sieciowej w postaci przełączników 10/25/40/100 Gigabit Ethernet tworzących sieć o architekturze „IP fabric" (spine/leaf) i znajdujących się pod wyłączną kontrolą komponentu zarządzającego SDN.

12.2. Funkcjonalność architektury systemu SDN i komponentu zarządzającego (kontrolera SDN):

a) Kontroler SDN jest zrealizowany w oparciu o dedykowaną warstwę sprzętową i programową. Zasoby sprzętowe (CPU, pamięć, dyski, porty sieciowe) są w pełni dedykowane dla oprogramowania kontrolera SDN,
b) Kontroler SDN zrealizowany jest redundantnie zarówno w warstwie sprzętowej jak i programowej tak, aby zapewnić spójne działanie środowiska i możliwość modyfikacji konfiguracji po ewentualnej utracie jednej z instancji.
c) Utrata wszystkich instancji kontrolera SDN nie wpływa na działanie infrastruktury sieciowej w zakresie istniejącej konfiguracji (nie dotyczy to zmian konfiguracji),
d) Komunikacja między kontrolerem SDN i elementami infrastruktury sieciowej (tzw. „IP fabric") jest możliwa w trybie in-band, niewymagającym użycia dedykowanych interfejsów na przełącznikach wchodzących w skład architektury,
e) Kontroler SDN obsługuje wyłącznie ruch związany z zarządzaniem i monitorowaniem infrastruktury sieciowej (tzw. „control plane"), nie zajmuje się przełączaniem ruchu (tzw. „data plane"),
f) Kontroler SDN umożliwia zarządzanie infrastrukturą sieciową złożoną z 2000 portów i dołączającą co 500 fizycznych serwerów dwuprocesorowych (odpowiednie licencje, jeśli wymagane, muszą być dostarczone na docelową pojemność platformy),

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

g) Kontroler SDN umożliwia zarządzanie infrastrukturą wirtualną złożoną z 2000 maszyn wirtualnych VM (odpowiednie licencje, jeśli wymagane, muszą być dostarczone na docelową pojemność platformy).

12.3. Funkcjonalność SDN dla oprogramowania komponentu zarządzającego (kontrolera SDN):

a) Umożliwia automatyzację konfiguracji zarządzanej sieci w oparciu o model sieciowych polityk powiązanych z aplikacjami,

b) Polityka definiowana na kontrolerze opisuje model działania aplikacji w oparciu o relacje pomiędzy punktami styku elementów aplikacji z siecią. W przykładowym modelu trójwarstwowym aplikacji oznacza to:
   - Zdefiniowanie warstw aplikacji takich jak web, aplikacyjna i bazodanowa (Web, App, DB),
   - Zdefiniowanie przydziału serwera wirtualnego do danej warstwy aplikacyjnej/segmentu na bazie jego atrybutów – nazwa maszyny VM, id maszyny VM, nazwa systemu operacyjnego, tagi itp.,
   - Zdefiniowanie relacji pomiędzy warstwami aplikacyjnymi, jako wzajemnie udostępnianych i konsumowanych zasobów opisanych przez polityki bezpieczeństwa (filtracji oraz przekierowania na zewnętrzne urządzenia bezpieczeństwa),

c) Umożliwia zintegrowanie usług zewnętrznych poprzez zapewnienie mechanizmu przekierowania ruchu dla warstw 4-7 dla funkcjonalności Next Generation Firewall,

d) Dla izolowanych środowisk sieciowych SDN umożliwia implementację funkcjonalności dedykowanej bramy wyjściowej L3 oraz dedykowanych usług zewnętrznych realizowanych dla warstw 4-7,

e) Realizuje tworzenie segmentów sieci L2 i L3 w oparciu o technologię VXLAN,

f) Realizuje sprzętowy VTEP,

g) Umożliwia monitorowanie i diagnostykę sieciową dla uruchamianych środowisk w oparciu o następujące mechanizmy:
   - Prezentację sprawności środowiska/aplikacji w formie wskaźnika stanu zdrowia,
   - Prezentowanie bieżącej i historycznej statystyki ruchu dla danego środowiska sieciowego,
   - Diagnostykę ścieżki (traceroute) między dowolną parą portów fizycznych bądź wirtualnych wchodzących w skład infrastruktury,
   - Monitorowanie i raportowanie ilości wykorzystanych i dostępnych zasobów wchodzących w skład infrastruktury,
   - Monitorowanie ruchu poprzez kopiowanie (mirroring) ruchu dla wybranych warstw aplikacyjnych lub interfejsów sieciowych,
   - Umożliwia automatyczną detekcję topologii oraz inwentarza infrastruktury sieciowej. Dopuszcza się realizację na innym komponencie zarządzania pod warunkiem zapewnienia dedykowanej, redundantnej platformy sprzętowej,
   - Implementuje centralne repozytorium oprogramowania (firmware) dla infrastruktury sieciowej. Dopuszcza się realizację na innym komponencie

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

zarządzania pod warunkiem zapewnienia dedykowanej, redundantnej platformy sprzętowej,

- Implementuje centralny mechanizm aktualizacji oprogramowania (firmware) dla infrastruktury sieciowej. Zamawiający dopuszcza realizację na innym komponencie zarządzania pod warunkiem zapewnienia dedykowanej, redundantnej platformy sprzętowej,
- Udostępnia interfejs zarządzania poprzez GUI,
- Integracja z Active Directory,
- Udostępnia następujące mechanizmy programowania (alternatywa do GUI):
  - ✓ REST API ze wsparciem dla formatu XML,
  - ✓ Możliwość konfiguracji infrastruktury bezpośrednio poprzez HTTP (np. z wykorzystaniem Postman REST Client),
  - ✓ Python SDK,
  - ✓ Powszechnie dostępna dokumentacja dla REST API,
- Udostępnia autoryzację dostępu użytkowników w oparciu o mechanizmy LDAP lub lokalne definicje,
- Umożliwia synchronizację całej infrastruktury sieciowej w oparciu o protokół NTP.

12.4. Funkcjonalność sprzętowa dla infrastruktury sieciowej („IP fabric") pozostającej pod nadzorem komponentu zarządzającego (kontrolera SDN):

a) Złożona z przełączników 10/25/40/100 GigabitEthernet, zorganizowanych w dwustopniowej nieblokowalnej architekturze rdzeń-brzeg (spine-leaf) określanej jako „IP fabric",

b) Przełączniki są wspierane i zarządzane przez komponent zarządzający (kontroler SDN) opisany powyżej,

c) Zarządzana jako całość poprzez centralny komponent zarządzający (kontroler),

d) Wszystkie połączenia między warstwą brzegową i rdzeniową w ramach fabric implementowane są jako 100GE o pełnej wydajności (wirespeed) z wykorzystaniem interfejsów QSFP i połączeń 100GE opartych o jednoparowe okablowanie single i multi mode LC,

e) Implementuje następujące protokoły i mechanizmy L2:
   - Sprzętowe wsparcie dla VXLAN Bridging i VXLAN Routing w oparciu o sprzętowy VTEP,
   - Dołączanie urządzeń zewnętrznych (serwerów, modułów, przełączników) poprzez zagregowaną wiązkę połączeń LACP 802.3ad do dwóch przełączników brzegowych (multi link aggregation, virtual port channel, itp.),
   - Pełna mobilność serwera fizycznego i wirtualnego w domenie L2, również pomiędzy kilkoma DC,
   - Definiowanie zewnętrznych połączeń w domenie L2,
   - Mechanizm eliminacji pętli na przełącznikach brzegowych w IP Fabric,

f) Implementuje następujące protokoły i mechanizmy L3:
   - IPv4 Unicast i Multicast,

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

- Przesyłanie IPv6 Unicast,
- Niezależne sieci prywatne (VRF) z duplikacją adresacji IP,
- Protokoły routingu eBGP, iBGP, OSPF dla IPv4 i IPv6,
- Routing statyczny dla IPv4 i IPv6,
- Przełączanie ruchu pomiędzy parą podsieci IP (SVI) realizowane sprzętowo w modelu IP Anycast w ramach fabric tj. na każdym przełączniku brzegowym, niezależnie od ilości przełączników brzegowych w fabric,
- Pełna mobilność serwera fizycznego i wirtualnego w domenie L3,
- Interfejsy i subinterfejsy L3 (per VLAN) na portach fizycznych przełączników brzegowych,
- Definiowanie zewnętrznych połączeń w domenie L3 opartych o protokoły routingu statycznego lub dynamicznego (OSPF lub BGP),

g) Implementuje następujące mechanizmy optymalizacji ruchu:
- Load-balancing pakietów dostosowany się do różnych warunków przesyłania (natłoku) w ramach środowiska opartego o ECMP,
- Priorytetyzacja połączeń.

12.5. Aplikacja dbająca o stan infrastruktury SDN z następującą funkcjonalnością:

a) Analiza na bieżąco zdarzeń i logów celem identyfikacji znanych ostrzeżeń, ich wpływu na określone przełączniki urządzenia, oraz zalecenia dotyczące działań naprawczych

b) informacje o błędach, podatnościach (PSIRT/CVE), zaleceniach producenta, poprawkach, EOL / EOS oprogramowania i sprzętu

c) Anomalie w konfiguracji – informacje o przekroczeniu przez konfiguracje zweryfikowanej skali

d) Informacje o problemach w utwardzeniu platformy, niezgodnościach w warstwie zarządzania (np. w bazie danych konfiguracji)

e) Informacja o wpływie poprawek na dostępność systemu - czy aktualizacja oprogramowania będzie bezprzerwowa lub nie / czy (nowy) sprzęt może obsługiwać istniejący zestaw funkcji i skalę

f) Otwieranie zgłoszeń u dostawcy wraz ze wsparciem przygotowania i dostarczenia wymaganych logów.

g) Aplikacja wspierająca analizę problemów w rozwiązaniu SDN:
- Analityka zdarzeń
  - ✓ Zbieranie danych: zmiany konfiguracji, zdarzenia i błędy w w warstwie zarządzania
  - ✓ Analiza z wykorzystaniem AI/ML (uczenie maszynowe) celem określenia korelację między wszystkimi zmianami, zdarzeniami i błędami.
  - ✓ Wykrywanie anomalii: z wykorzystaniem AI/ML detekcja nieoczekiwanych zdarzeń, w tym tych mających wpływ na przestoje.
- Wizualizacja wykorzystania zasobów, z podziałem na następujące kategorie:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

- ✓ Zasoby operacyjne: Wyświetla pojemność zasobów, które mają charakter dynamiczny i oczekuje się ich zmiany w krótkich odstępach czasu. Przykładami są trasy, adresy MAC, tablice zabezpieczeń (ACL) itp.
- ✓ Zasoby konfiguracyjne: Wyświetla wykorzystanie pojemności zasobów zależnych od konfiguracji, takich jak liczba VRF, VLAN, (mikro)segmentów itp.
- ✓ Zasoby sprzętowe: wykorzystanie ilości portów i przepustowość.

– Środowiskowe (temperatura, utylizacja CPU, RAM, prędkości wentylatorów itp.)
– Analityka przepływów – celem identyfikacji anomalii sieciowych i ich źródeł w warstwie transmisji (data plane). Wspierane anomalie: odrzucone pakiety, opóźnienia, ruchy, przemieszczenia workload (MAC itp), problemy z routingiem, odrzucone pakiety/ramki przez ACL.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706