Agenţia de Administrare a Reţelei Naţionale de Informatică pentru Educaţie şi Cercetare
Str. Mendeleev 21-25, Sector 1, 010362
Bucureşti – România
www.nren.ro
Tel./Fax: +40-21-3171175

APROB,
DIRECTOR GENERAL,
DINU GHEORGHE

Nr .1711 din data de 8 octombrie 2018

CAIET DE SARCINI

Prezenta procedură de achiziție publică are ca obiect atribuirea contractului de furnizare şi implementare a sistemului informatic integrat (numit în continuare, platforma) de tip Campus Şcolar Wireless, pe baza prevederilor prezentului caiet de sarcini şi a documentației de achiziție respectiv publicate de autoritatea contractantă.

Descrierea cerințelor şi caracteristicilor tehnice şi nontehnice precum şi a condițiilor de realizare a platformei sunt descrise în cele ce urmează.

1. OBIECTIVELE PROIECTULUI

1.1. Introducere

Practica internațională a consacrat accesul, de oriunde și oricând, la resurse de date și servicii digitale, prin rețele locale interconectate și în Internet, ca necesitate de zi cu zi, pentru o cât mai mare parte a categoriilor socio-profesionale și a grupelor de vârstă, pentru ca societatea modernă să beneficieze cu adevărat de pe urma avantajelor pe care acestea le oferă.

Pe măsură ce utilizarea tehnologiei a devenit parte a vieții de zi cu zi, s-au dezvoltat atât metodele și practicile de utilizare eficientă a acesteia, cât și, pe de altă parte, așteptările în ceea ce privește implicarea tehnologiei în tot mai multe aspecte ale vieții personale, profesionale și ale interacțiunii sociale.

Tehnologia informației și comunicațiile, cu precădere comunicațiile mobile, fără fir, ocupă un loc cu totul special în preocupările tinerei generații, inclusiv ale copiilor și tinerilor de vârstă școlară, și prezintă un potențial excepțional în contextul modernizării procesului educațional.

1.2. Necesitatea proiectului

Studii moderne estimează că, până în 2020, la nivel global, prezența în mediul online va ocupa un loc cu totul special în procesul de dezvoltare cognitivă, de formare a personalității lor și a aptitudinilor specifice de angajare și de integrare socială, pentru un număr de peste 700M de copii cu vârste de 8-12 ani, din care 90% din țările cu o dezvoltare avansată a tehnologiei IT.

Pornind de la afinitatea manifestă a tinerelor generații pentru utilizarea tehnologiei informației, cu precădere a aplicațiilor de comunicare și colaborare de pe terminale mobile inteligente, s-a creat oportunitatea creării unui mediu adecvat, care să răspundă rigorilor și nevoilor specifice procesului educațional, dar care să sprijine și dezvoltarea armonioasă a relației copiilor și tinerilor între ei și cu societatea, prin mijlocirea utilizării tehnologiei dar și, în egală măsură, a relației lor cu tehnologia, ca parte integrantă a procesului educațional.

În mod realist, recuperarea distanței crescânde, în ultimele decenii, între tinerele generații și rezervorul neprețuit de civilizație pe care cartea (și, în sens mai larg, artefactul cultural și științific) îl reprezintă, respectiv menținerea și dezvoltarea intreresului copiilor de vârstă școlară și a tinerilor pentru școală, pentru învățare, se poate realiza numai în condițiile înțelegerii rolului pe care trebuie să îl joace tehnologia în acest proces.

Crearea unui mediu dedicat vieții școlare, cu precădere la nivelul școlilor gimnaziale, pentru comunicare și colaborare, care să întâlnească interesul elevilor pentru utilizarea tehnologiei moderne cu posibilitățile pe care le oferă o rețea școlară de tip campus, conectată la rețele deschise și Internet, va avea un efect decisiv în sprijinirea misiunii școlii românești de a forma și dezvolta noile generații.

În ultimii ani, o dată cu dezvoltarea tehnologiei, a crescut mult numărul dispozitivelor inteligente care se pot conecta la servicii digitale și, în general, la Internet, prin metode de comunicații radio (wireless) și cu suport pentru mobilitate, și care pot fi folosite în procesul educațional, în același timp în care a scăzut semnificativ costul marginal al punerii în operă de infrastructuri tehnice și funcționale specifice pentru acestea.

Astfel, accesul la resurse și servicii digitale prin utilizarea tehnologiei informației și a comunicațiilor devine o resursă esențială în procesul de predare-învățare, putând facilita gestiunea comunicării și a colaborării, dezvoltarea creativității și accesul la informație prin dispozitive mobile inteligente (de exemplu: telefoane și calculatoare portabile în format tabletă sau laptop), iar beneficiile se transpun în îmbunătățirea eficienței și eficacității procesului educațional la toate nivelurile, atât în cadre formale cât și informale.

În prezent, există acces limitat la resurse digitale proprii școlii și, de asemenea, acces limitat la Internet în școli (de exemplu: numai în laboratoarele de informatică), iar acest fapt îngreunează accesul elevilor și al cadrelor didactice la serviciile și la resursele educaționale online existente și compromite dezvoltarea utilizării resurselor și a interacțiunii online ca resursă critică a procesului educațional modern.

Conform Programului Operațional Competitivitate (POC) 2014-2020, se evidențiază tipurile de intervenții prin care se are în vedere dezvoltarea infrastructurii TIC în școli, inclusiv *îmbunătățirea accesului la Internet prin implementarea de platforme de tip Campus Școlar Wireless, cu prioritate în școlile gimnaziale.*

Realizarea Platformei naționale integrate Campus Școlar Wireless ("Campus-WiFi"), se constituie practic într-o premisă operațională cheie (*prerequisite*) pentru realizarea potențialului celorlalte mecanisme de intervenție.

Proiectul va permite școlii românești să valorifice oportunitatea de a folosi asigurarea accesului protejat la rețele deschise de comunicații, cu precădere de pe terminale mobile inteligente, atât pentru a spori atractivitatea procesul educațional și motivația elevilor, cât și pentru diversificarea și eficientizarea

metodelor de interacțiune între elevi, între elevi și profesori și, nu în ultimul rând, a interacțiunii cu părinții elevilor.

1.3. Obiectivele proiectului

Pentru asigurarea serviciului de acces fără fir (wireless, în tehnologie WiFi), la rețele de date deschise inteconectate, inclusiv la Internet, proiectul va crea componenta de infrastructură proprie de comunicații a strategiei de îmbunătățire a accesului la resurse educaționale în format digital, ca rețea națională cu prezență în școli de nivel gimnazial și cu acces la Internet, administrată centralizat de la nivelul regional și central de management găzduit de infrastructura rețelei naționale educaționale (RoEduNet).

Astfel, se va crea un mediu coerent integrat, administrat și protejat centralizat pentru a răspunde nevoilor specifice utilizării susținute și coerente a comunicației convergente, pentru acces la resurse de date (inclusiv conținut multi-media) de interes educațional și la serviciile de aplicație asociate, ca resurse critice pentru procesul educațional modern și astfel se vor pune bazele utilizării pe scară largă a unor modele și metode educaționale moderne și flexibile, care să faciliteaze și să susțină învățarea.

Obiectivul general al proiectului îl reprezintă crearea unei platforme naționale integrate de tip campus care va asigura, cu prioritate în școli de nivel gimnazial, serviciul de acces fără fir la rețele de date deschise interconectate, inclusiv la Internet.

Obiectivele specifice ale proiectului sunt:

- Crearea infrastructurii tehnice necesare utilizării resurselor și serviciilor de tip OER și WEB 2.0 în educație la minim 2000 de școli la finalul implementării proiectului

- Dotarea în cadrul proiectului a unui număr de 4.500 de unități gimnaziale cu echipamente wireless, prin implementarea proiectului

- Creșterea ponderii profesorilor ce utilizează internetul prin wireless-campus la 15% la finalul perioadei de sustenabilitate a proiectului

2. CERINȚE PRIVIND SOLUȚIA TEHNICĂ

2.1. Cerințe generale

În diagrama de mai jos este prezentată arhitectura sistemului, pe bază de niveluri funcționale, care definesc amplasarea fizică şi regruparea zonală a componentelor platformei de tip campus național, la cel mai înalt nivel de abstractizare a organizării acesteia.

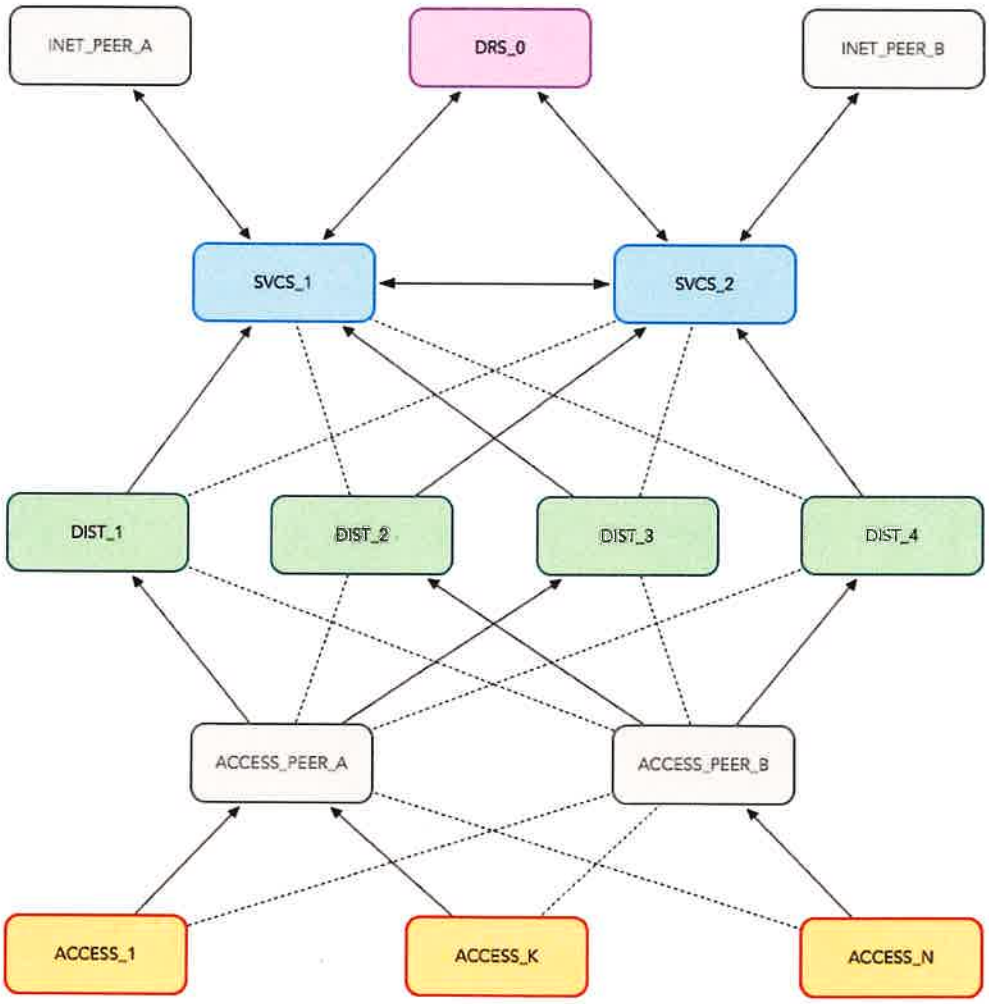

Diagrama (0) — Arhitectura de nivel înalt a platformei

Cerințele specifice reflectă rolul şi conținutul fiecărei componente funcționale, care asigură regruparea logică a funcționalităților cheie ale soluției, respectiv descompunerea structurală a arhitecturii acesteia.

Pentru fiecare componentă funcțională, sunt incluse cerințe funcționale obligatorii, precum și cerințe specifice de echipare, de capacitate și de performanță maxim suportate pentru componentele soluției tehnice de implementare a proiectului (scalabilitatea soluției preconizate).

Proiectul tehnic organizează cerințele pentru soluția tehnică respectiv pe baza următoarei structuri:

- Context și rol, care identifică contextul respectiv relevant, pentru fiecare componentă funcțională, și rolul specific al acesteia, în ansamblul proiectului.
- Cerințe generale, pentru fiecare componentă funcțională în parte, respectiv aplicabile ansamblului livrabilelor componentei, sau unor anume livrabile specific identificate, inclusiv:
    - Cerințe de capabilitate, respectiv în forma unor funcționalități disponibile, ca atare, în configurația preconizată a soluției sau, exclusiv în cazurile în care se prevede în mod explicit această posibilitate, sunt suportate prin licențiere software suplimentară și/sau prin adăugare de componente hardware;
    - Cerințe de scalabilitate, respectiv în forma unor criterii de minim specific aplicabile — acolo unde acestea sunt relevante — nivelurilor de echipare, de capacitate și de performanță din configurațiile maxim suportate de livrabilele componentei;
    - Alte cerințe, respectiv specific relevante pentru soluția tehnică de implementare a proiectului, dar care nu se regăsesc în categoriile definite mai sus.

De la caz la caz, pentru fiecare componentă și, respectiv, pentru fiecare livrabil în parte, cerințele generale au fost incluse în măsura în care s-au dovedit necesare pentru a defini în mod specific substanța tehnic-funcțională a acestora pentru necesitățile proiectului.

Pentru atingerea obiectivelor asumate de proiect se impune asigurat un nivel adecvat de interoperabilitate între livrabile, respectiv coeziunea internă a fiecărei componente, între acestea și, pe ansamblu, viabilitatea operațională a platformei.

Specificațiile tehnice și de dimensionare sunt regrupate pe structura de livrabile tehnice și asimilate, care inventariază componența soluției și asigură corespondența între organizarea documentației tehnice și organizarea bugetului de proiect.

Pentru fiecare livrabil sunt incluse specificații tehnice și de dimensionare, precum și specificații de echipare, de capacitate și de performanță efectiv asigurate în configurația minim acceptabilă (soluția ce va fi achiziționată).

Specificațiile tehnice și de dimensionare, pentru livrabilele soluției tehnice, sunt organizate pe baza următoarei structuri:

- Dimensionarea soluției, care reunește cerințe specifice pentru dimensionarea cantitativă a soluției, respectiv exprimate ca număr de unități din fiecare livrabil (cantitate), precum și definirea unităților de măsură respectiv aplicabile.
- Specificații tehnice pentru configurația oferită, acolo unde acestea sunt considerate relevante în contextul proiectului, pentru a defini nivelurile efective de echipare, de capacitate și de performanță ale livrabilelor componentei, în configurația oferită.

2.2. Protecția datelor și securitate

2.2.1. Managementul accesului la sistem

Arhitectura platformei va permite segregarea nivelului regional de distribuție și a nivelului central de servicii, prin mijloace de zonare indepedentă a rețelei și prin măsuri de autorizare explicită, inclusiv la nivel de aplicație, a accesului administrativ.

Se va asigura un nivel înalt de autentificare (inclusiv de tip multi-factor) și control explicit al accesului utilizatorilor cu rol administrativ la resursele platformei, pe baza configurării specifice a funcționalităților relevante ale componentelor de alocare a resurselor de adresare la nivel de rețea (IPAM/DNS) și de autentificare, autorizare și audit (AAA).

De asemenea, pe baza configurării celor două componente, se va asigura posibilitatea înregistrării prealabile a terminalelor pentru acces la platformă, respectiv autentificarea și autorizarea accesului acestora la serviciile platformei, care va putea fi realizată atât în mod transparent, cât și în mod explicit.

Platforma va permite organizarea terminalelor autorizate în funcție de rolul lor, și al utilizatorilor acestora (de exemplu, între dispozitivele folosite de personalul didactic și administrativ, pentru acces privilegiat la resurse și funcții ale serviciilor educaționale, inclusiv de tipul catalogului electronic, și dispozitivele client folosite de elevi), sau după grupe de vârstă și profile de interes educațional, respectiv definire proactivă și aplicarea consecventă a politicilor de acces corespunzătoare.

2.2.2. Confidențialitatea datelor

Datele generate și stocate de platformă vor fi stocate în sistem numai în formă criptată și vor putea fi accesate numai prin intermediul aplicațiilor și al serviciilor de management respectiv relevante, numai de către personalul specific autorizat, numai după autentificare și în condiții de asigurare permanentă a mijloacelor și a informației martor de audit, și numai în funcție de nevoia de a cunoaște definită pentru fiecare tip/rol de acces.

2.2.3. Securitatea sistemului

Tehnologia aleasă va permite atestarea și conservarea integrității componentelor funcționale cheie, inclusiv de la nivel de pre-boot, iar arhitectura preconizată va asigura protecția transparentă anti-malware a resurselor generale și protecția explicită, inclusiv prevenirea accesului neautorizat, în cazul resurselor tehnic-administrative și a datelor stocate în sistem.

Se vor utiliza funcționalitățile de filtrare și de control activ al utilizării acceptabile a accesului la rețele deschise, pe specificul și pentru nevoile procesului educațional, și în scopul de a ridica nivelul general al securității sistemului, în sensul limitării posibilității ca accesul normal la Internet — menit să asigure accesul la resurse, conținut digital și servicii educaționale — să nu faciliteze, inclusiv accidental, accesul extern neautorizat la resursele platformei și acțiunea codului neautorizat (de tip malware, sau asimilat).

Se vor asigura niveluri funcționale independente de protecție transparentă a accesului autorizat la rețele deschise și de protecție explicită a resurselor administrative, astfel:

- Cel puțin la nivelul echipamentelor Router de Tip 2, parte a Componentei de dirijare a traficului și interconectrare WAN, se va asigura capacitatea de zonarea a rețelei și de separare a zonelor definite ca interne platformei și a resurselor externe acesteia, controlul traficului între acestea, precum și protecția zonelor definite prin mecanisme integrate de tip firewall;
- Cel puțin la nivelul echipamentelor Gateway de protecție, parte a Componentei de protecție a rețelei private de serviciu, se va implementa protecția independentă a echipamentelor și a serviciilor de management al platformei și, în mod specific al funcțiilor (inclusiv IPAM/DNS, AAA) asociate asigurării accesului la resursele interne în Campus, în rețele deschise externe și în Internet.
- Cel puțin prin funcționalitățile Componentei de alocare a resurselor de adresare la nivel de rețea se va asigura și protecția activă împotriva atacurilor specifice serviciilor de tip IPAM/DNS.
- Cel puțin prin funcționalitățile Componentei de retenție a datelor de audit se va asigura valorificarea informației de audit generate de sistem pentru monitorizarea operațională și de securitate a platformei.

3. DESCRIEREA COMPONENTEI TEHNICE A PROIECTULUI

3.1. Arhitectura funcțională a sistemului

3.1.1. Nivelul local de acces

Nivelul local de acces regrupează 4500 puncte de prezență (PoP-uri) de acces, câte unul la nivel de școală.

Diagrama de mai jos identifică punctele de prezență de acces — PoP Acces, numerotate de 1 la 4500 — și poziționarea acestora în arhitectura platformei:

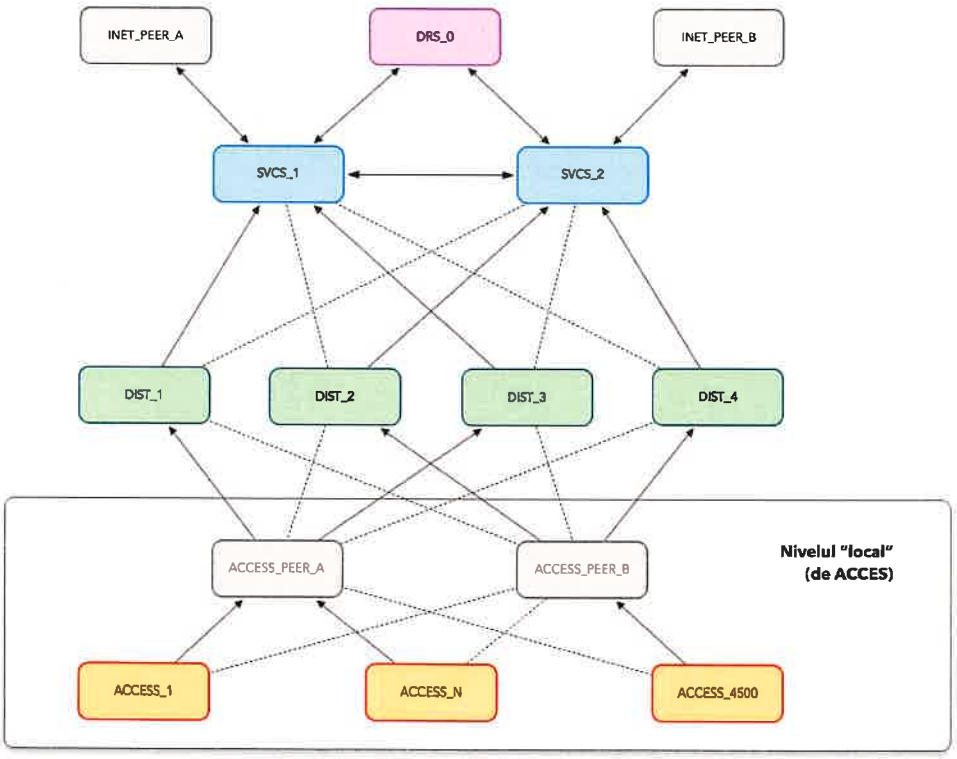

Diagrama (1) — Nivelul local de ACCES

3.1.2. Nivelul regional de distributie

Nivelul regional de distributie regrupează (cel puțin) 4 puncte de prezență (PoP-uri) pentru servicii de distribuție.

Diagrama de mai jos identifică punctele de prezență de distribuție — PoP Distribuție, numerotate de la 1 la (cel puțin) 4 — și poziționarea acestora în arhitectura platformei:

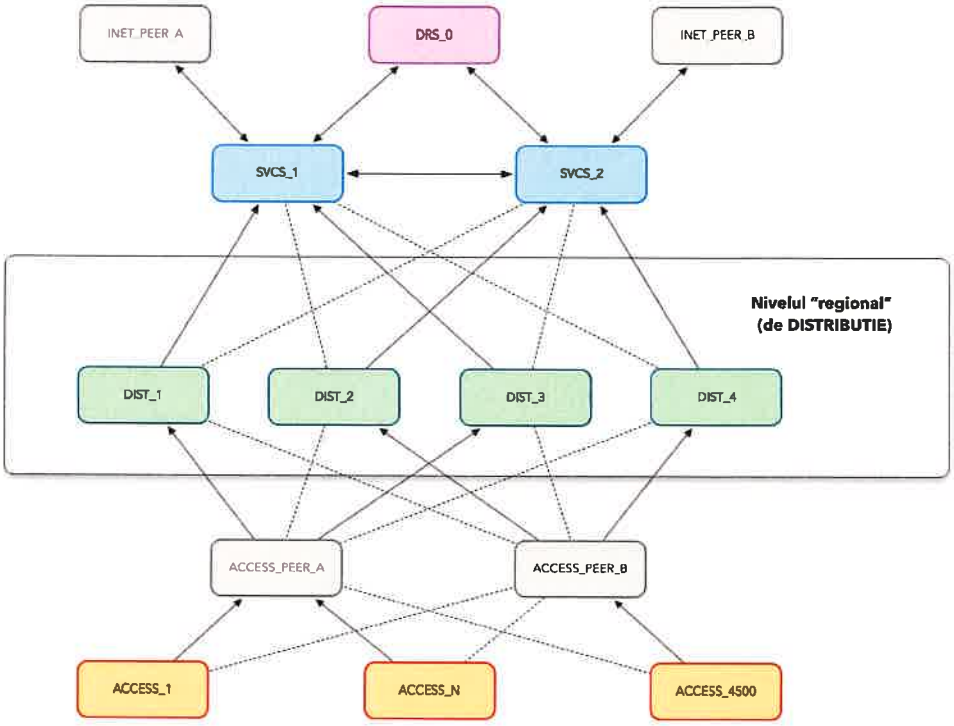

Diagrama (2) — Nivelul regional de DISTRIBUTIE

3.1.3. Nivelul central de servicii

Nivelul central de servicii regrupează (cel puțin) 2 puncte centrale de prezență (PoP-uri) de servicii de acces la Internet și, respectiv, (cel puțin) 1 punct central de prezență (PoP) de servicii de DR (disaster recovery și capacități de rezervă).

Diagrama de mai jos identifică punctele centrale de prezență pentru servicii de tip gateway de acces la Internet (IGS) — PoP Servicii IGS_1 și Servicii PoP IGS_2 — și punctele centrale de prezență pentru asigurarea capacităților de rezervă și servicii de tip disaster recovery (DRS) — PoP Servicii DRS_0 —, precum și poziționarea acestora în arhitectura platformei:

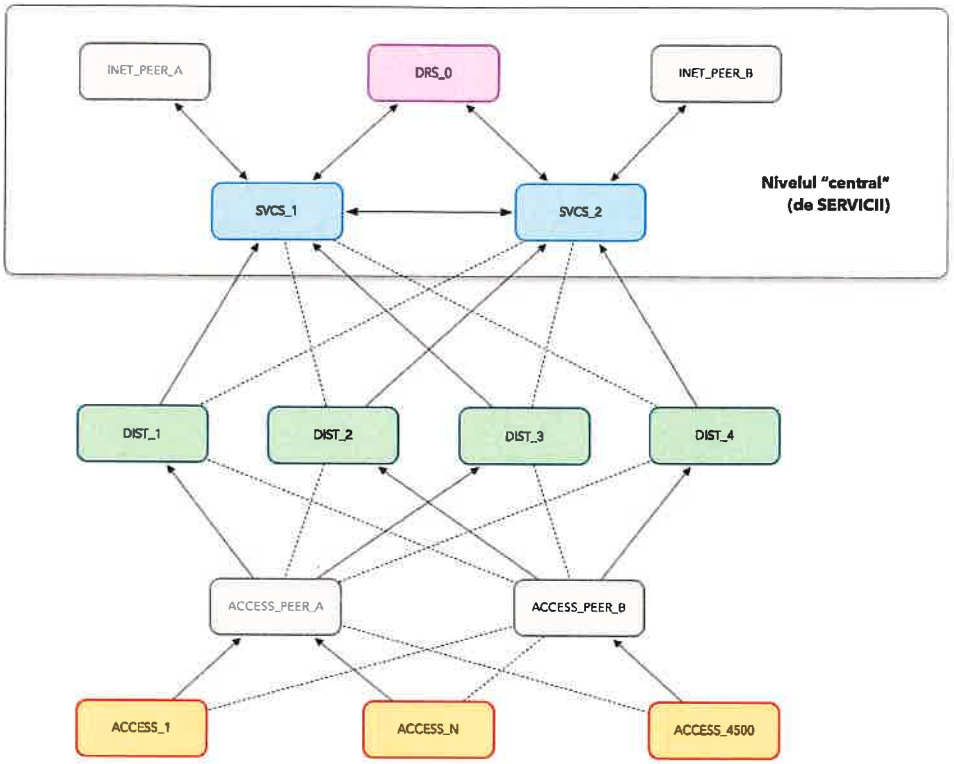

Diagrama (3) — Nivelul central de SERVICII

3.2. Cerințe specifice pentru soluția tehnică

3.2.1. Componenta de acces primar în tehnologie Wi-Fi

Context și rol

Componenta (cod C-I) asigură funcționalitățile de acces local wireless, în tehnologie Wi-Fi, inclusiv controlul accesului la serviciu exclusiv pentru terminalele înregistrate şi autorizate.

Componenta de acces primar Wi-Fi este alcatuită din următoarele tipuri de echipamente, respectiv definite la capitolul Specificații tehnice şi dimensionare:

- Echipamente de tip AP Wi-Fi (cod APW).

  Bucla locală de acces wireless, în tehnologie Wi-Fi, la nivel de școală.

Diagrama de mai jos introduce livrabilele componentei de acces primar în tehnologie Wi-Fi şi poziționarea acestora în arhitectura platformei:

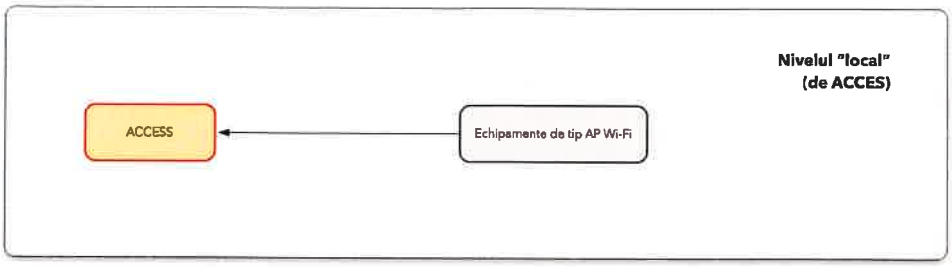

Diagrama (4) — Componenta de acces primar Wi-Fi

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Importanța interoperabilității cu serviciile IPAM/DNS (legătura cu C-VIII) și AAA (legătura cu C-IX) pentru a garanta alocarea transparentă a resurselor de adresare, pentru terminalele autorizate care accesează platforma prin intermediul echipamentelor de tip AP Wi-Fi, și auditarea eficientă a utilizării acestora.
- Necesitatea asigurării funcționalităților de administrare a echipamentelor din infrastructura de bază prin aceeași componcntă funcțională a platformei (legătura cu C-VII).

Cerințe generale

Echipamentele de tip AP Wi-Fi trebuie să asigure suport nativ pentru tehnologie Wi-Fi de ultimă generație, respectiv cel puțin pentru standardul IEEE 802.11ac Wave2.

Echipamentele de tip AP Wi-Fi trebuie să dispună de mai multe interfețe radio, și să poată fi configurate să opereze în spectru radio atât în banda de 2.4GHz, cât și în banda de 5GHz.

Echipamentele de tip AP Wi-Fi trebuie să asigure suport pentru protejarea comunicațiilor, inclusiv prin mijloace criptografice standard, între terminalele client conectate și echipamentele de tip AP Wi-Fi.

Echipamentele de tip AP Wi-Fi trebuie să poată fi alimentate direct din echipamentele de tip switch de interconectare LAN pentru nivelul de acces (SW1A/C-III și SW1B/C-III) în tehnologie PoE+, conform standardului IEEE 802.3at.

Având în vedere rolul esențial al buclei locale wireless, în tehnologie Wi-Fi, ca parte a serviciilor de bază ale platformei, se va asigura independența îndeplinirii funcțiilor de controller de existența conectivității între școală și nivelul de distribuție și servicii.

Pentru a elimina nevoia de a administra individual fiecare echipament de tip AP Wi-Fi se va asigura managementul centralizat al acestora prin funcționalități de tip controller local Wi-Fi și se vor asigura, în acest sens, cel puțin următoarele:

- Configurarea integrală a dispozitivelor de tip AP Wi-Fi din cadrul fiecărei școli (cel puțin pentru configurarea inițială, modificări ulterioare ale configurației de bază, implementarea și configurarea de functionalități suplimentare, upgrade-uri de software/firmware inclusiv pentru rezolvarea anumitor probleme de securitate);
- Alocarea dinamică și administrare resurselor radio (bandă, canale, putere), în cursul exploatării platformei, în mod centralizat, la nivel de școală.
- Scalabilitate adecvată și posibilitatea de fail-over automat pe un alt echipament din cadrul aceluiasi punct de acces, pentru asigurarea administrării directe a tuturor echipamentelor de tip AP Wi-Fi din cadrul școlii;
- Vizibilitate sasupra aplicațiilor folosite, prin inspecția pachetelor (în AP sau controller), inclusiv cu funcționalități de detecție și de clasificare, și posibilitatea controlului, restricționării și prioritizării (inclusiv limitarea utilizării aplicațiilor consumatoare de resurse de bandă), pentru asigurarea unui nivel adecvat de performanță;
- Optimizarea utilizării și protejarea rețelei wireless, pentru fiabilitate și performanța, inclusiv prin detectarea interferențelor Wi-Fi, precum și suprimarea echipamentelor Wi-Fi străine instalate si conectate in scoală;
- Indicatori vizuali de stare.

Pentru a asigura integritatea funcțională a întregii infrastructuri și confidențialitatea datelor transportate peste aceasta, echipamentele de tip AP Wi-Fi trebuie să implementeze mecanisme de verificare a autenticității sistemului de operare instalat.

Dimensionarea specifică a Componentei de acces primar în tehnologie Wi-Fi este dată la pct. 3.3.1, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.2. Componenta de dirijare a traficului și de interconectare WAN

Context și rol

Componenta (cod C-II) asigură interconectarea punctelor de prezență de acces, din școlile înrolate în platformă, cu nivelul de distribuție și cu nivelul de servicii, din PoP-urile RoEduNet, respectiv dirijarea

traficului peste rețele deschise intermediare și Internet, precum și protejarea traficului prin crearea de structuri de tunelare și prin anvelopa criptografică aplicată.

Componenta de dirijare a traficului și de interconectare WAN este alcatuită din următoarele tipuri de echipamente, respectiv definite la capitolul Specificații tehnice și dimensionare:

- Router de Tip 1A (cod R1A);
  Echipamente (de tip router integrat multi-serviciu) de dirijare a traficului și de interconectare WAN, la nivel de acces.
- Router de Tip 1B (cod R1B);
  Echipamente (de tip router integrat multi-serviciu) de dirijare a traficului și de interconectare WAN, la nivel de acces.
- Router de Tip 2 (cod R2);
  Echipamente (de tip router integrat multi-serviciu) de dirijare a traficului și de interconectare WAN, la nivel de distribuție.
- Router de Tip 3A (cod R3A);
  Echipamente (de tip router de acces la Internet, cu funcții CGN) de dirijare a traficului și de interconectare WAN, la nivel central, în centrele principale de servicii.
- Router de Tip 3B (cod R3B).
  Echipament de dirijare a traficului și de interconectare WAN, la nivel central, în centrul de rezervă.

Diagrama de mai jos introduce livrabilele componentei de dirijare a traficului și de interconectare WAN și poziționarea acestora în arhitectura platformei.

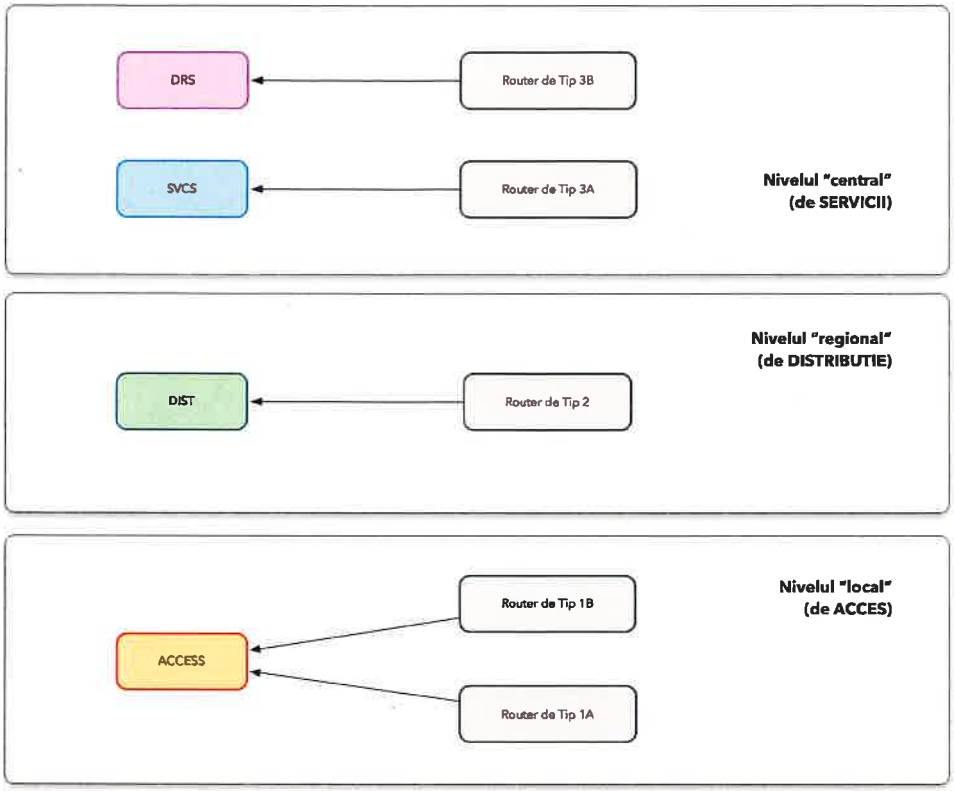

Diagrama (5) — Componenta de dirijare a traficului şi de interconectare WAN

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea asigurării funcționalităților de administrare a echipamentelor din infrastructura de bază prin aceeaşi componentă funcțională a platformei (legătura cu C-VII);
- Compatibilitatea necesară, la nivelul componentei (coeziunea internă a C-II), între livrabilele implicate în crearea logicii de tunelare a traficului şi în aplicarea anvelopei criptografice de protecție a caracterului privat al traficului din platformă, cel puțin între nivelul de acces şi cel de distribuție.

Cerințe generale

În nivelul de acces, Componenta de dirijare a traficului şi de interconectare WAN include echipamentele Router de Tip 1A şi 1B, care vor asigura cel puțin:

- Conectarea printr-o tehnologie de WAN, cu suport pentru criptare de ultima generatie (cel putin AES256), la echipamentele din nivelul de distribuție, folosind conectivitatea existentă în şcoală;

- Dirijarea traficului, pentru terminalele client înrolate și autorizate, conectate la celelalte echipamente de acces din școală (de tip AP Wi-Fi sau Switch);

De asemenea, echipamentele de tip router din nivelul de acces trebuie să poată oferi o separare completă a traficului între tipuri diferite de clienți (identificabile și prin subinterfețe logice cu corespondență în structurile de tip VLAN definite în infrastructura de interconectare din nivelul de acces), prin functionalități de tip VRF sau echivalente.

O alta facilitate necesară este funcționalitatea de QoS, care să ofere administratorului posibilitatea de a prioritiza anumite tipuri de trafic pentru fiecare profil de utilizator, respectiv asociat cu fiecare terminal autorizat, atât în zona de rețea WAN, cât și în zona de retea de acces LAN.

Pentru asigurarea posibilității de configurare și utilizare de conexiuni de rezervă și de management de tip 3G/4G/LTE, echipamentele Router de Tip 1A și 1B trebuie să suporte cel puțin standardul LTE 2.0 în implementare care să fie compatibilă cu rețelele operatorilor din România și, de asemenea, compatibil cu standardele precendente, precum: DC-HSPA+, HSPA+, HSPA, UMTS, EDGE și GPRS.

Conexiunea de tip 3G/4G/LTE trebuie să poată fi activată automat în cazul în care conexiunea principală la Internet nu mai functionează, dar să poată fi și utilizată simultan cu aceasta. Routerul trebuie să poată utiliza simultan conexiunea principală (existentă în școală) și conexiunea 3G/4G/LTE inclusiv pentru a transmite și recepționa date prin conexiunea VPN către nivelul de distribuție.

Funcția de protecție a accesului la Internet are ca scop asigurarea, de la nivelul echipamentelor Router de Tip 1A și 1B, a navigării în siguranță, în condiții compatibile cu specificul procesului educațional și în conformitate cu politica de folosire a rețelei, respectiv printr-o funcționalități de tip filtrare URL cu urmatoarele caracteristici:

- Sa analizeze tot traficul de tip Web ce tranziteaza routerul și să identifice destinația pentru a permite filtrarea;
- Sa permită filtrarea traficului pe baza unui set extins de categorii predefinite, selectabile și a căror aplicare să fie configurabilă centralizat dintr-o interfață unică pentru toate locatiile din nivelul Acces;
- Să permită filtrarea traficului pe baza reputației site-urilor catalogate, cel puțin prin asocierea a 3 categorii reputaționale de bază, respectiv: sigur, riscant, malign;
- Cataloagele de categorii și de asociere a indicatorilor de reputație a site-urilor catalogate trebuie să poată fi actualizate permanent, centralizat, în mod automat și fără a fi necesară intervenția administratorului.

Cel puțin echipamentele Router de Tip 2 vor implementa funcții de bază pentru protecția rețelei, de tip (zone-based) firewall, care vor asigura protecției transparente implicite împotriva prezenței și a acțiunii malware, la nivel de rețea, și vor împiedica inițierea neautorizată de conexiuni către echipamentele client conectate la Campus din afara acesteia.

Cel puțin echipamentele Router de Tip 2 trebuie să dețină capabilitatea nativă de a furniza date de telemetrie referitoare la întreg traficul care a tranzitat echipamentul, date ce vor include: adresa IP sursă, adresa IP destinație, port sursă, port destinație, protocol TCP/UDP, TOS, interfața logică de intrare

Pentru a asigura integritatea funcțională a întregii infrastructuri și confidențialitatea datelor transportate peste aceasta, echipamentele Router de Tip 1A, 1B, 2, 3A si 3B trebuie să implementeze mecanisme de verificare a autenticității sistemului de operare instalat, respectiv care nu va permite decât utilizarea unei imagini software semnate digital de producător.

Dimensionarea specifică a Componentei de dirijare a traficului și de interconectare WAN este dată la pct. 3.3.2-6, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.3. Componenta de interconectare LAN pentru serviciile de bază ale platformei

Context și rol

Componenta (cod C-III) asigură interconectarea locală LAN, în fiecare punct de prezență și pentru toate nivelurile arhitecturii platformei, în regim de switching L2, a porturilor de serviciu ale echipamentelor (respectiv a celor care expun, față de utilizatorii platformei și față de celelalte echipamente ale acesteia, funcționalitățile care contribuie la furnizarea serviciilor de bază ale platformei).

Componenta de interconectare LAN pentru serviciile de bază ale platformei este alcatuită din următoarele tipuri de echipamente, respectiv definite la capitolul Specificații tehnice și dimensionare:

- Switch de Tip 1A (cod SW1A);
  Echipamente de interconectare (de tip Switch Ethernet 1G) la nivel local, în rack.
- Switch de Tip 1B (cod SW1B);
  Echipamente de interconectare (de tip Switch Ethernet 1G) la nivel local, pe etaj, pe DIN-rail.
- Switch de Tip 2 (cod SW2);
  Echipamente de interconectare (de tip Switch Ethernet 10G) la nivel regional și central.
- Switch de Tip 3 (cod SW3);

Echipamente de interconectare (de tip Switch Ethernet 40G) la nivel regional și central.
Diagrama de mai jos introduce livrabilele componentei de interconectare LAN pentru serviciile de bază ale platformei și poziționarea acestora în arhitectura platformei.

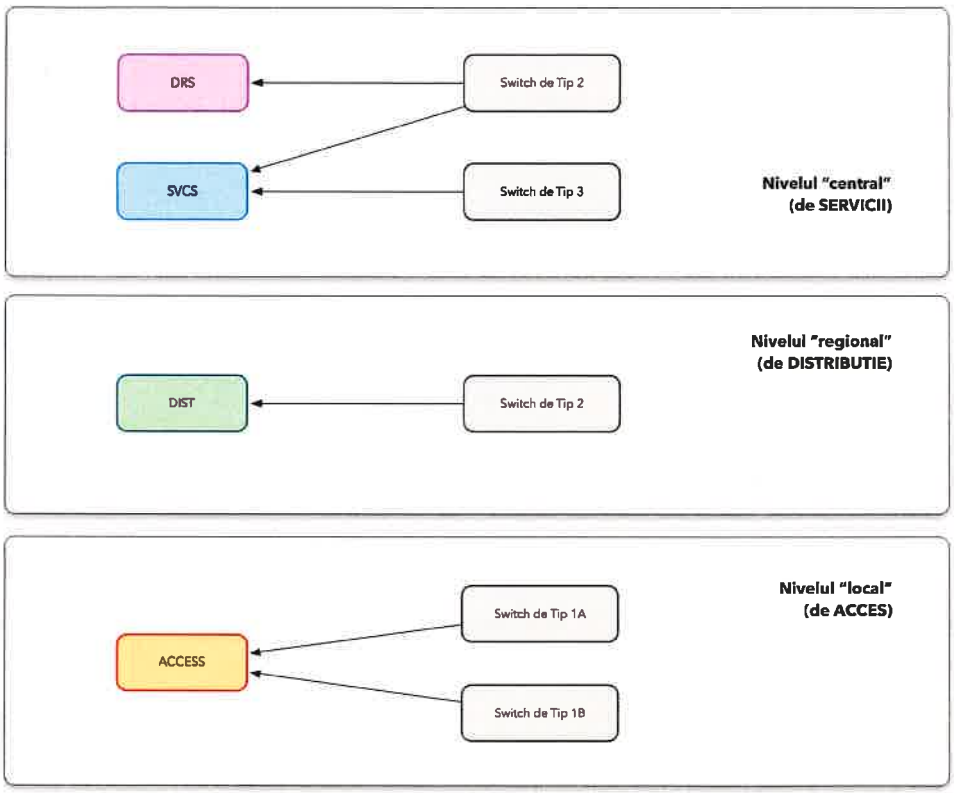

Diagrama (6) — Componenta de interconectare LAN pentru serviciile de bază ale platformei

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea asigurării funcționalităților de administrare a echipamentelor din infrastructura de bază prin aceeași componentă funcțională a platformei (legătura cu C-VII).

Cerințe generale

Livrabilele Switch de Tip 1A (SW1A) și de tip 1B (SW1B) din nivelul de acces se vor baza pe o platformă funcțională comună, vor oferi un design compact și flexibilitate în ceea ce privește opțiunile de montare, în rack standard sau în incinte de tip industrial, pe șine DIN (sau echivalent), și vor asigura

premisele de fiabilitate în exploatare, în condițiile date, cel puțin prin răcirea echipamentului fără ventilare mecanică (fără a utiliza piese în mișcare).

Pentru a asigura disponibilitatea operațională a serviciului de buclă locală Wi-Fi, trebuie ca echipamentele Switch de Tip 1A și 1B să asigure alimentarea echipamentelor de tip AP Wi-Fi deservite, prin funcționalitate PoE+, conform standardului IEEE 802.3at.

Este necesar ca echipamentele Switch de tip 1A și 1B să suporte mecanisme de separare a traficului (segmentarea logică a rețelei locale de acces) și mecanisme pentru a conecta în mod controlat zonele astfel definite.

Pentru a asigura un nivel adecvat de securitate în zona de acces, echipamentele Switch de Tip 1A și 1B vor dispune de mecanisme specifice ce vor contracara disfunctionalitățile ce pot fi cauzate de conectarea locală a unui server DHCP neautorizat sau de atacuri de tip "IP spoofing" sau "MAC spoofing", atacuri ce sunt relativ usor de efectuat de pe un laptop conectat local, în switch. Aceste mecanisme de protectie vor fi disponibile atât pentru IPv4 cât și pentru IPv6.

Pentru a asigura integritatea funcțională a întregii infrastructuri și confidențialitatea datelor transportate peste aceasta, echipamentele Switch de Tip 1A și 1B trebuie să implementeze mecanisme de verificare a autenticității sistemului de operare instalat, respectiv care nu va permite decât utilizarea unei imagini software semnate digital de producător.

Pentru a asigura premisele unui consum rațional de energie electrică, în mod specific pentru perioadele fără trafic activ cum ar fi nopțile, zilele nelucratoare sau perioadele de vacanță, echipamentele Switch de tip 1A și 1B trebuie să asigure și un mod de operare low-power (de tip hibernare), configurabil centralizat, fără a fi necesar accesul fizic, în acest scop, la echipament.

Dimensionarea specifică a Componentei de interconectare LAN pentru serviciile de bază ale platformei este dată la pct. 3.3.7-10, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.4. Componenta de interconectare LAN pentru funcțiile de management

Context și rol

Componenta (cod C-IV) asigură interconectarea locală LAN, în fiecare punct de prezență și pentru nivelurile de distribuție și de servicii din arhitectura platformei, în regim de switching L2, a porturilor de management ale echipamentelor (respectiv a porturilor prin care se accesează, de către utilizatorii

specific autorizați, direct sau prin intermediul componentelor dedicate de management, funcționalitățile de configurare și de administrare tehnică a echipamentelor și/sau a instanțelor platformei).

Componenta de interconectare LAN pentru serviciile de bază ale platformei este alcatuită din următoarele tipuri de echipamente, respectiv definite la capitolul Specificații tehnice și dimensionare:

- Switch de Tip 4 (cod SW4).
  Echipamente de interconectare a porturilor și interfețelor private (dedicate) de management al echipamentelor din infrastructura platformei.

Diagrama de mai jos introduce livrabilele componentei de interconectare LAN pentru funcțiile de management și poziționarea acestora în arhitectura platformei.

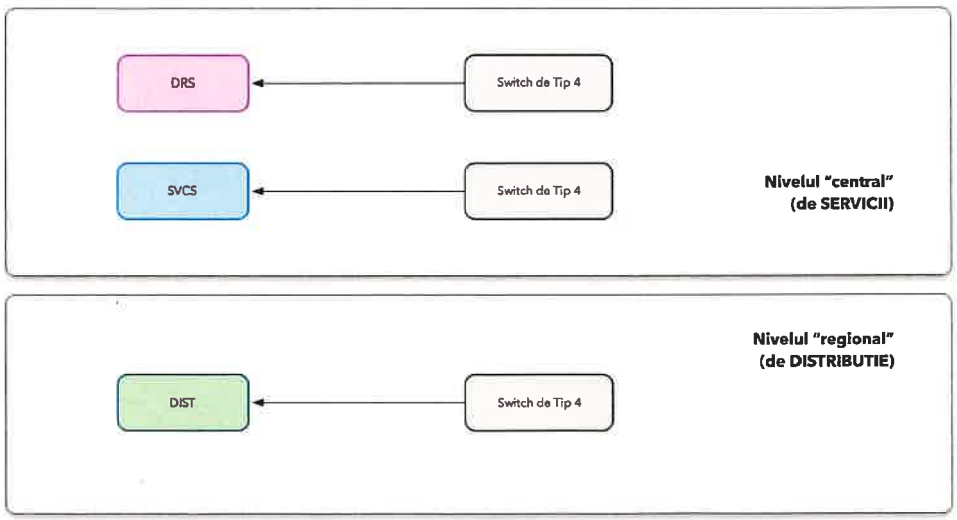

Diagrama (7) — Componenta de interconectare LAN pentru funcțiile de management

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea asigurării funcționalităților de administrare a echipamentelor din infrastructura de bază prin aceeași componentă funcțională a platformei (legătura cu C-VII).

Cerințe generale

Pentru a asigura integritatea funcțională a întregii infrastructuri și confidențialitatea datelor transportate peste aceasta, echipamentele de tip SW4 trebuie să implementeze mecanisme de verificare a

autenticității sistemului de operare instalat, respectiv care nu va permite decât utilizarea unei imagini software semnate digital de producător.

Dimensionarea specifică a Componentei de interconectare LAN pentru funcțiile de management este dată la pct. 3.3.11, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.5. Componenta de interconectare LAN/SAN pentru funcțiile suport de back-end

Context și rol

Componenta (cod C-V) asigură interconectarea privată LAN/SAN, în punctele principale de prezență ale nivelului central de servicii, în regim de switching Ethernet și FC, a echipamentelor de back-end (respectiv a acelora care asigură suportul de procesare și de stocare pentru instanțele centrale active virtualizate de tip server, atât a celor care contribuie la furnizarea serviciilor de bază ale platformei, cât și a celor care asigură funcțiile de management ale acesteia).

Componenta de interconectare LAN/SAN pentru funcțiile suport de back-end este alcatuită din următoarele tipuri de echipamente, respectiv definite la capitolul Specificații tehnice și dimensionare:

- Switch de Tip 5 (cod SW5).
  Echipamente (de tip port- sau fabric-extender) de interconectare privată convergentă (LAN/SAN) pentru nivelul central de servicii.

Diagrama de mai jos introduce livrabilele componentei de interconectare LAN/SAN pentru funcțiile suport de back-end și poziționarea acestora în arhitectura platformei.

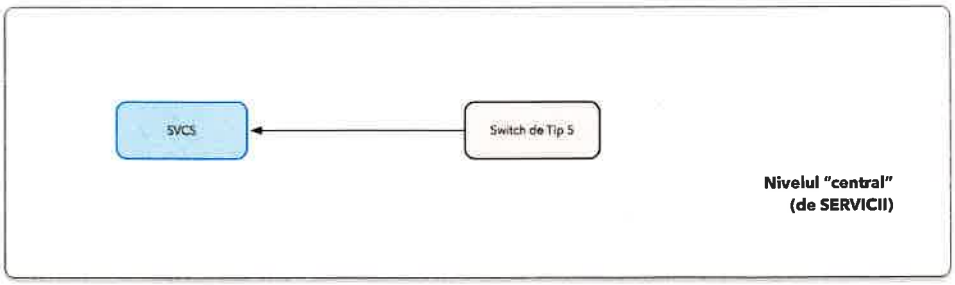

Diagrama (8) — Componenta de interconectare LAN/SAN pentru funcțiile suport de back-end

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea asigurării compatibilității cu livrabilele componentei de infrastructură IT de uz general (legătura cu C-VI), echipamente de stocare și procesare, la nivel central, în punctele de prezență de servicii de acces la Internet.

Cerințe generale

Pentru a asigura integritatea funcțională a întregii infrastructuri și confidențialitatea datelor transportate peste aceasta, echipamentele de tip SW5 trebuie să implementeze mecanisme de verificare a autenticității sistemului de operare instalat, respectiv care nu va permite decât utilizarea unei imagini software semnate digital de producător.

Dimensionarea specifică a Componentei de interconectare LAN/SAN pentru funcțiile suport de back-end este dată la pct. 3.3.12, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.6. Componenta de infrastructură IT pentru funcțiile de management

Context și rol

Componenta (C-VI) asigură instanțelor active virtualizate de tip server (atât a celor care contribuie la furnizarea serviciilor de bază ale platformei, cât și a celor care asigură funcțiile de management ale acesteia) suportul integrat hardware și software (cel puțin la nivel de hipervizor, pentru virtualizarea funcțiilor de sistem și de rețea) pentru procesarea sarcinilor de aplicație și de management, precum și a funcțiilor de stocare a datelor.

Componenta de infrastructură IT de uz general pentru funcțiile de management este alcatuită din următoarele tipuri de echipamente, respectiv definite la capitolul Specificații tehnice și dimensionare:

- Echipamente de procesare de Tip 1 (cod EP1);
  Echipamente (de tip server) pentru susținerea instanțelor de servicii, la nivel local.
- Echipamente de procesare și stocare de Tip 2 (cod EP2);
  Echipamente (de tip hiper-convergent) pentru susținerea instanțelor de servicii, la nivel de distribuție și în centrul de rezervă (la nivel central).
- Echipamente de procesare de Tip 3 (cod EP3);
  Echipamente (de tip server modular "blade") pentru susținerea instanțelor de servicii, în centrele active de servicii (la nivel central).
- Echipamente de stocare de Tip 1 (cod ES1).

Echipamente de stocare tranzacțională (de performanță) pentru susținerea instanțelor de servicii, în centrele active de servicii (la nivel central).

Diagrama de mai jos introduce livrabilele componentei de infrastructură IT de uz general pentru funcțiile de management și poziționarea acestora în arhitectura platformei:

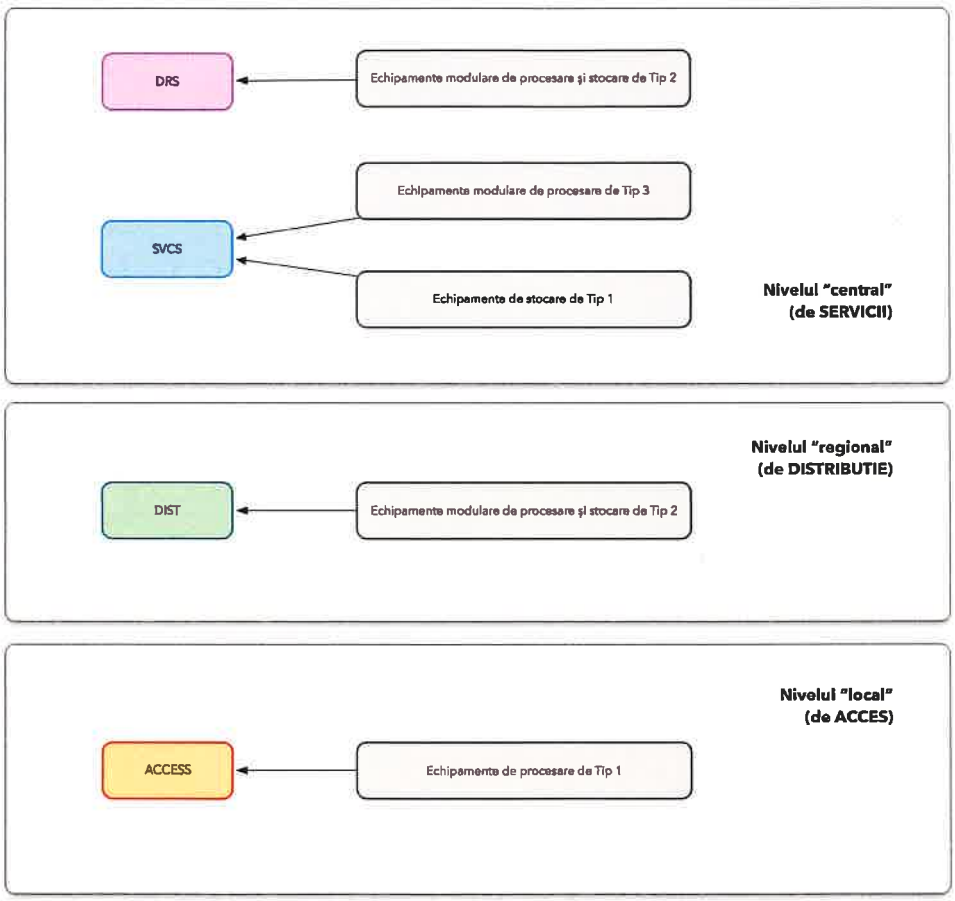

Diagrama (9) — Componenta de infrastructură IT de uz general

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea asigurării compatibilității cu livrabilele componentei de interconectare LAN/SAN pentru funcțiile suport de back-end (legătura cu C-V), la nivel central, în punctele de prezență de servicii de acces la Internet.

- Necesitatea asigurării compatibilității cu livrabilele componentei de retenție a datelor (legătura cu C-XI), la nivelul centrelor de servicii, pentru stocarea și accesarea copiilor de rezervă (*disaster recovery*) ale instanțelor virtualizate.

Cerințe generale

La nivelul Echipamentelor de procesare de Tip 1 se vor asigura:

- Funcționalități de virtualizare incluse, cel puțin la nivel de hipervizor de tip 1 (suportă instalare nativă bare metal), care va putea susține rularea de instanțe locale de servicii de management (inclusiv, după necesități, de alocare a resurselor de adresare la nivel de rețea și/sau de tip AAA).
- Capabilitatea de administrare (inclusiv la nivel de acces administrativ, la nivel de consolă KVM, de la distanță).

La nivelul Echipamentelor de procesare și de stocare de Tip 2 se vor asigura:

- Funcționalități de virtualizare și de management incluse, pentru asigurarea implementării logicii de tip HCI (infrastructură hiper-convergentă, cu nivel de procesare, de stocare și de rețea virtualizate, definite software);
- Capabilități de management proactiv al funcției de stocare, de optimizare integrată a utilizării capacității de stocare instalate, precum și de protejare a datelor stocate, inclusiv prin utilizarea de mijloace criptografice.
- Capabilitatea de efectuare a instalării de pachete corective și de upgrade în mod consolidat și simplificat (single-click), pentru funcționalitățile software și firmware (hardware) ale platformei HCI, între stări stabile ale sistemului;
- Mecanisme de management centralizat al sistemului (clusterului) HCI, cel puțin la nivel de site, care să includă configurarea și monitorizarea consolidată a nodurilor, precum și capacitatea de a genera și de a utiliza imagini de rezervă (snapshot) și de siguranță (back-up) pentru instanțele active care rulează pe echipament;
- Cel puțin conectivitate 10Gbps Ethernet în front-end, pentru acces tranzacțional de la nivelul clienților de serviciile instalate pe platformă;

La nivelul Echipamentelor de procesare de Tip 3 se vor asigura:

- Funcționalități de virtualizare și de management centralizat incluse, pentru asigurarea implementării logicii de tip SDDC (infrastructură virtualizată de tip centru de date, cu nivel de procesare și de rețea virtualizate, definite software) și care se vor putea integra și cu funcționalitățile Echipamentelor de stocare de tip 1, pentru a asigura nivelul funcțional de virtualizare a funcției de stocare;

- Platforma de virtualizare trebuie permită reconfigurarea resurselor de procesare (inclusiv memoria activă) și de stocare fără restartarea sistemului de operare din mașina virtuală;
- Pentru instanțele virtualizate din centrele de servicii se va asigura posibilitatea generării și utilizării de copii de rezervă locale și un regim de reziliența (HA/DR) multi-site, inclusiv prin integrarea funcționalităților de virtualizare licențiate pe echipamentele de procesare cu cele ale echipamentelor de stocare de Tip 1.
- Cel puțin conectivitate 10/40Gbps CNA (Ethernet/FC), pentru interconectare privată cu Echipamentele de stocare de Tip 1 și, respectiv, pentru access tranzacțional de la nivelul clienților la serviciile instalate pe platformă;
- Pentru instanțele virtualizate din centrele de servicii se va asigura posibilitatea generării și utilizării de copii de rezervă locale și un regim de reziliența (HA/DR) multi-site, inclusiv prin integrarea funcționalităților de virtualizare licențiate pe echipamentele de procesare cu cele ale echipamentelor de stocare de Tip 1.

La nivelul Echipamentelor de stocare de Tip 1 se vor asigura:

- Pentru fiecare punct de prezență, o structură cluster de tip scale-out format din perechi de unități active de tip controller, în care toate unitățile de tip controller din cluster vor opera în mod activ-activ, în arhitectură de tip *no single point of failure*.
- Suport integrat pentru serviciu de stocare consolidată, care va putea aloca flexibil resursele disponibile, ca discuri virtuale, în arhitectură SAN, pentru toată capacitatea instalată și care va putea proteja datele stocate, inclusiv prin mijloace criptografice;
- Capacitate nativă de generare a copiilor de siguranță de tip snapshot, în puncte de consistență, pentru funcții de backup/recovery, cu suport nativ pentru platforme uzuale de virtualizare, de gestiune a bazelor de date și de aplicații;
- Integrare la nivel API cu funcționalitățile de management al stocării oferite de soluția de virtualizare licențiată pe Echipamentele de procesare de Tip 3, precum și cu instanțele centrale de management general al acesteia.
- Funcții integrate de compresie și deduplicare automată de date care să opereze inline, în timp real și la nivel global — pentru întreaga capacitate de stocare asigurată, inclusiv pentru datele reținute ca parte a copiilor de siguranță de tip snapshot —, precum și capacitate de supra-alocare nominală (thin provisioning) a capacității instalate;
- Unități interne de stocare amovibile, exclusiv în tehnologie SSD de tip enterprise (componente optimizate pentru performanță individuală), care vor rezista la cel puțin 3-5 cicluri de scriere/ștergere pe zi, pe durata de viață;

- Timp de răspuns specific liniar sub 1ms, în mod independent de sarcina de I/O deservită, în condiții realiste de încărcare (efort tranzacțional susținut variabil, între minim și maxim suportat);
- Un mediu privat de back-end, de tip fabric redundant Infiniband, Ethernet, FC (sau echivalent), pentru interconectarea unităților de tip controller și partajarea metadata între toate nodurile active în cluster;
- Posibilitatea de update și upgrade al elementelor software al platformei fără întreruperea serviciului, pentru asigurarea unui nivel optim de disponibilitate operațională, precum și creşterea capacității maxime de stocare prin adăugarea și reconfigurarea de componente hardware, fără a fi necesară ștergerea sau migrarea datelor stocate existente.
- Funcționalități integrate, care să asigure o interfață unică de control și de gestiune centralizată a sistemului de stocare, care va putea fi accesată inclusiv folosind API-uri de tip REST, cu posibilitate de monitorizare și de administrare a configurării și reconfigurării, a alertelor specifice și a metricilor de performanță.
- Cel puțin conectivitate 16Gbps FC și 10Gbps iSCSI în front-end, pentru acces tranzacțional de la nivel de host/server.

Dimensionarea specifică a Componentei de infrastructură IT pentru funcțiile de management este dată la pct. 3.3.25-28, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.7. Componenta de management general al infrastructurii de bază

Context și rol

Componenta (cod C-VII) asigură funcționalitățile de configurare și de administrare generală a infrastructurii de bază, respectiv a echipamentelor și a instanțelor virtualizate care susțin serviciile de bază ale platformei și include consola centrală de administrare.

Infrastructura de bază platformei include (cel puțin) echipamentele de tip AP Wi-Fi și echipamentele de tip switch de interconectare LAN pentru nivelul de acces, precum și echipamentele de tip router, de la nivel de acces și distribuție, până la nivelul funcțional de servicii de tip gateway de acces la Internet.

Componenta de management general al infrastructurii de bază este alcatuită din următoarele livrabile:

- Server de management de Tip 1 (cod SM1);
  Echipamentele/instanțele de management (element management) al echipamentelor din infrastructura de bază.

- Consola de management de Tip 1 (cod CM1).

  Consola centrală pentru funcțiile de (element) management.

Diagrama de mai jos introduce livrabilele componentei de management general al infrastructurii de bază și poziționarea acestora în arhitectura platformei.

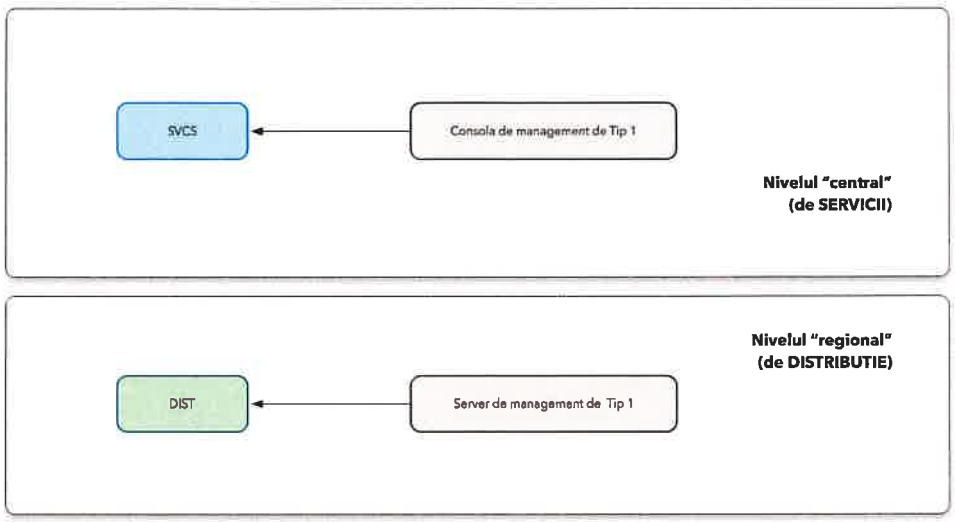

Diagrama (10) — Componenta de management general al infrastructurii de bază

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea asigurării suportului pentru echipamentele din infrastructura de bază (cel puțin legătura cu C-I , C-II și C-III) pentru care această componentă asigură managementul.

Cerințe generale

Componenta de management general al infrastructurii de bază va asigura cel puțin:

- Managementul configurațiilor echipamentelor de rețea;
- Managementul si update-ul sistemelor de operare ale echipamentelor de retea;
- Posibilitatea de definire a unor hărți ierarhice pentru diferite arii geografice, clădiri si etaje;
- Inventarierea echipamentelor de rețea, cel puțin în funcție de tip, identificare (numere de serie) și echipare;
- Managementul performanței generale a echipamentelor de rețea și monitorizarea alarmelor asociate acestora;

- Vizualizarea încărcării spectrului RF, în fiecare punct de prezență, și a parametrilor de performanță ai echipamentelor;
- Monitorizarea starii rețelei și a clientilor asociați, din punct de vedere al defecțiunilor, configurației si performanței.

Se vor asigura functionalități de raportare, care să ofere cel puțin:

- Sabloane predefinite de rapoarte, incluzând rapoarte de resurse și inventar, rapoarte de analiză, rapoarte de tip trend, top-N și rapoarte pentru defecte;
- Crearea, modificare, ștergerea, vizualizarea online, exportarea și generarea periodică a rapoartelor;
- Posibilități de personalizare a rapoartelor, inclusiv gruparea mai multor rapoarte într-unul singur;
- Trimiterea de notificari sub forma de email după generarea unui raport;
- Exportul rapoartelor în format CSV sau PDF.

Se vor asigura rapoarte predefinite care să ofere cel puțin:

- Inventarul echipamentelor wireless existente în rețea (acces point-uri, controlere), care să poată fi generat pentru fiecare categorie hardware sau ca un raport combinat pentru toate categoriile;
- Performanta echipamentelor, cel puțin la nivel de utilizare a memoriei și a procesorului, precum și zonele care prezintă deficit de acoperire wireless.
- Informații despre echipamentele neautorizate din rețea, detectate de fiecare acces point.

Se va asigura posibilitatea de definire a unor domenii virtuale de administrare și alocarea de roluri cu permisiuni diferite pe grupuri distincte de echipamente pentru a permite alocarea unor drepturi de administrare corespunzatoare anumitor administratori.

Pentru facilitarea administrarii de la nivel central a echipamentelor EP1, parte a infrastructurii de bază, componenta funcțională va fi configurată și licențiată (dacă soluția presupune licențiere de activare a funcționalităților, a capacității și/sau a performanței solicitate) pentru a asigura cel puțin:

- O interfata unică centralizată în care să prezinte informații despre echipamentele EP1 (inclusiv procesoare, memorii, dispozitive PCI, controllere RAID, fisiere de log) precum si despre erori si alarme;
- Posibilitatea de a executa diverse acțiuni asupra echipamentelor EP1 (inclusiv pornire, oprire, lansarea consolei KVM remote);
- Posibilitatea de a administra și upgrada centralizat firmware-ul de pe echipamentele EP1 și o interfată de tip REST/XML (sau echivalent) care să ofere acces la funcții mod programatic.

- Posibilitatea de a diagnostica de la distanta echipamentele EP1 și trimiterea prin email de notificari si rapoarte despre erorile prezente.

Dimensionarea specifică a Componentei de management general al infrastructurii de bază este dată la pct. 3.3.13-14, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.8. Componenta de alocare a resurselor de adresare la nivel de rețea

Context și rol

Componenta (cod C-VIII) asigură gestiunea alocării dinamice și monitorizarea utilizării efective a resurselor de adresare la nivel de rețea (adrese IP), asigură susținerea tranzacțională a serviciilor de IP Address Management (IPAM) și acelor de tip Domain Name Service (DNS), de translație între adresele Internet și descriptorii simbolici calificați de tip Fully Qualified Domain Name (FQDN), sau derivați, ai punctelor de acces la servicii, precum și protecția acestora împotriva atacurilor specifice.

Componenta de alocare a resurselor de adresare la nivel de rețea este alcatuită din următoarele tipuri de livrabile:

- Server de management de Tip 2 (cod SM2);
  Instanțe de serviciu IPAM/DHCP/DNS pentru echipamentele platformei campus și pentru terminalele client autorizate să acceseze platforma.
- Consola de management de Tip 2 (cod CM2).
  Consola centrală pentru funcțiile de IPAM/DHCP/DNS.

Diagrama de mai jos introduce livrabilele componentei de alocare a resurselor de adresare la nivel de rețea și poziționarea acestora în arhitectura platformei.

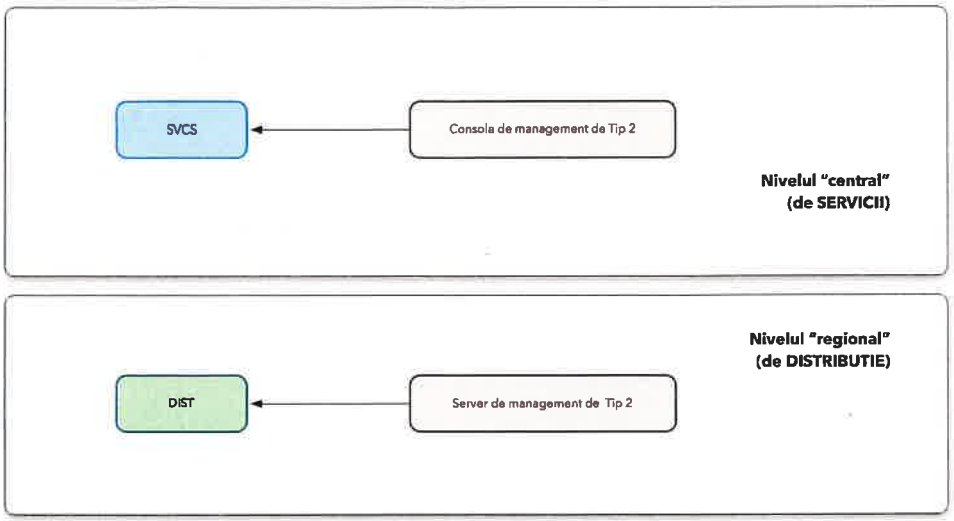

Diagrama (11) — Componenta de alocare a resurselor de adresare la nivel de rețea

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea integrării cu funcționalitățile de asigurare a accesului local wireless, în tehnologie Wi-Fi (legătura cu C-I), pentru coerența asigurării serviciului, inclusiv a controlul accesului la acesta exclusiv pentru terminalele înrolate în platformă;
- Necesitatea integrării cu componenta de autentificare, autorizare a accesului și audit curent (legătura cu C-IX), pentru asigurarea coerenței necesare între alocarea resurselor de adresare în rețea și autorizarea accesului pentru terminalele înrolate în platformă.

Cerințe generale

Prin Componenta de alocare a resurselor de adresare la nivel de rețea se vor asigura:

- Managementul centralizat al alocării resurselor de adresare disponibile (IPAM), atât pentru IPv4 cât și pentru IPv6.
- Management centralizat pentru serviciile de tip DNS și DHCP folosind o interfață de management unică.
- Posibilitatea configurării serviciilor de DHCP și DNS pe bază de modele (șabloane) predefinite.
- Monitorizarea alocării și utilizarii adreselor IP, corelarea utilizatorilor și a dispozitivelor folosite cu adresele IP respectiv utilizate.

- Vizibilitate completă în cererile efectuate către serviciul de DNS şi posibilitatea filtrării traficului ce poate fi asociat atacurilor cibernetice, inclusiv prin punerea în carantină a dispozitivelor sursă.
- Arhitectură scalabilă ce permite adaugarea de resurse suplimentare fără impact major asupra soluției instalate.
- Arhitectură multi-server şi multi-site distribuită, care să asigure un nivel ridicat de disponibilitate operațională.
- Posibilitatea implementării de fluxuri pentru modificările efectuate în sistemul de management.
- Posibilitatea planificării modificărilor de configurație necesare şi programarea efectuării acestora în perioadele de mentenanță.
- Posibilitatea limitării accesului la configurarea serviciilor pentru fiecare utilizator/administrator în parte.
- Suport pentru configurarea şi integrarea sistemului cu alte soluții şi servicii folosind servicii de tip API.

Dimensionarea specifică a Componentei de alocare a resurselor de adresare la nivel de rețea este dată la pct. 3.3.15-16, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare şi configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.9. Componenta de autentificare, autorizare a accesului şi audit curent

Context şi rol

Componenta (cod C-IX) asigură serviciile (de tip AAA) de autentificare, autorizare a accesului la serviciul de rețea şi de generare a informației martor de audit în ceea ce privește utilizarea acestuia, respectiv pentru a autentifica, permite şi audita accesul la servicii pentru terminalele înregistrate şi autorizate.

Componenta de autentificare, autorizare a accesului şi audit curent este alcatuită din următoarele tipuri de livrabile:

- Server de management de Tip 3 (cod SM3);
  Instanțe de AAA pentru accesul autorizat al terminalelor înregistrate.
- Consola de management de Tip 3 (cod CM3).
  Consola centrală de management pentru funcțiile de AAA.

Diagrama de mai jos introduce livrabilele componentei de autentificare, autorizare a accesului şi audit curent şi poziționarea acestora în arhitectura platformei.

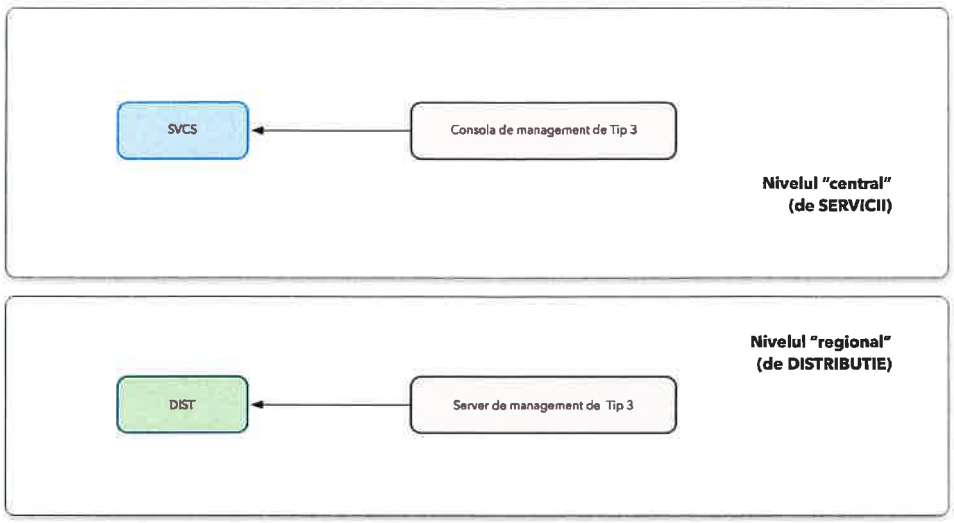

Diagrama (12) — Componenta de autentificare, autorizare şi audit curent al accesului

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea integrării, inclusiv în relație cu serviciile de IPAM/DNS (legătura cu C-VIII), cu funcționalitățile de asigurare a accesului local wireless, în tehnologie Wi-Fi (legătura cu C-I), pentru coerența asigurării serviciului, inclusiv a controlul accesului la acesta exclusiv pentru terminalele înrolate în platformă;
- Necesitatea integrării cu componenta de autentificare, autorizare a accesului şi audit curent (legătura cu C-VIII), pentru asigurarea coerenței necesare între alocarea resurselor de adresare în rețea şi autorizarea accesului pentru terminalele înrolate în platformă.

Cerințe generale:

Componenta de autentificare, autorizare a accesului şi audit curent are următoarele caracteristici

- Oferă o consolă grafică integrată de vizualizare a stării şi de configurare pentru toate elementele sale.
- Asigură un serviciu bazat pe protocolul RADIUS pentru autentificare şi autorizare, precum şi PAP, MS-CHAP, EAP sau diferite variante ale acestora.
- Asigură autoritate de certificare proprie sau integrare cu sisteme PKI existente şi oferă o consolă de management pentru certificatele utilizatorilor/terminalelor şi validarea lor folosind serviciul OCSP.

- Suportă configurarea flexibilă de politici de autentificare și autorizare bazate pe atribute ca numele utilizatorului, terminalul folosit, protocolul de autentificare sau alte atribute ce pot fi extrase din sesiune.
- Asigură posibilitatea integrării cu surse externe de informație de identitate precum LDAP, Microsoft Active Directory, ODBC sau alte servicii RADIUS.
- Asigură posibilitatea de a expune servicii de tip TACACS+ pentru controlul accesului la terminal, și de integrare la nivel SAML-2 cu servicii de tip identity/service provider;
- Pentru integrarea secvențelor de autentificare, de autorizare și de audit, soluția asigură funcționalități de tip server de autentificare centralizată, prin servicii transparente de RADIUS proxy și RESTful API.
- Acestea vor asigura posibilitatea de a utiliza, și direct și ca factor de autentificare suplimentară, dispozitivele mobile inteligente (cel puțin pentru iOS și Android) ce se vor conecta la platformă, respectiv de a utiliza dispozitive hardware standard de tip OATH TOTP (IETF RFC 6238) în lipsa acestora.
- Asigură posibilitatea asignării utilizatorilor într-un VLAN definit, pe baza politicii de acces predefinite.
- Asigură posibilitatea asignării de ACL-uri sau redirecționarea de URL-uri pentru utilizator, pe baza politicii de acces predefinite.
- Asigură posibilitatea integrării cu soluții de tip MDM/EMM pentru înrolarea și validarea avansată a terminalelor mobile.
- Asigură suport pentru predefinirea de șabloane pe baza tipului de terminal folosit și asocierea lor automată prin identificarea terminalului folosit.
- Asigură posibilitatea asocierii automate de politici de autorizare după identificarea terminalului folosit.
- Asigură suport pentru auditarea continuă a politicilor folosite la nivel de utilizator/terminal.
- Asigură suport pentru raportare în timp real sau la nivelul platformei sau pe baza auditului efectuat pentru fiecare utilizator în parte.

Oferta tehnică va prezenta detaliat fluxurile de lucru complete propuse, cu indicarea rolului componentelor platformei care asigură funcționalitățile relevante, cel puțin pentru înregistrarea terminalelor pentru acces autorizat la platformă, respectiv pentru autentificarea terminalelor și autorizarea accesului la rețea.

Soluția ofertată nu va presupune deținerea, de către personalul din școli, a unor cunoștințe speciale pentru determinarea elementelor selectate de identificare unică a terminalelor mobile, ca parte a procedurii de înregistrare a acestora în sistem.

Dimensionarea specifică a Componentei de autentificare, autorizare a accesului și audit curent este dată la pct. 3.3.17-18, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.10. Componenta de protectie a rețelei private de serviciu

Context și rol

Componenta (cod C-X) asigură protectia rețelei private de serviciu, în nivelurile de distribuție și de servicii, pentru definirea și aplicarea politicilor de acces autorizat normal la serviciile de management ale platformei, precum și împotriva situațiilor în care rețeaua privată de serviciu ar fi ținta unor atacuri informatice sau a utilizării abuzive datorită căreia platforma ar fi putea fi utilizată ca sursă de trafic de atac informatic îndreptat împotriva unor sisteme și rețele terțe.

Componenta de protectie a rețelei private de serviciu este alcatuită din următoarele tipuri de livrabile:

- Gateway de protectie de Tip 1 (cod GP1)
  Gateway de protecție a rețelei private de serviciu (în care se regăsesc echipamentele de configurare și de management al serviciului de acces la rețeaua campus și la internet al echipamentelor autorizate) la nivel de distribuție.
- Gateway de protectie de Tip 2 (cod GP2)
  Gateway de protecție a rețelei private de serviciu la nivel central, în centrul de rezervă.
- Gateway de protectie de Tip 3 (cod GP3)
  Gateway de protecție a rețelei private de serviciu la nivel central, în centrele active de servicii.
- Consola de management de Tip 4 (cod CM4)
  Consola centrală de management pentru funcțiile de protecție a rețelei private de serviciu.

Diagrama de mai jos introduce livrabilele componentei de protecție a rețelei private de serviciu și poziționarea acestora în arhitectura platformei.

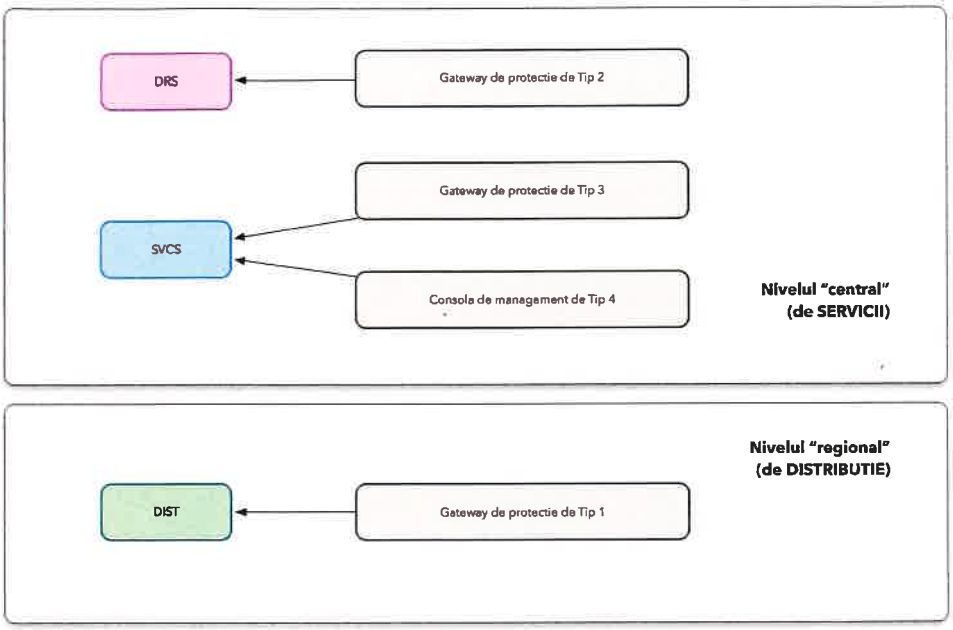

Diagrama (13) — Componenta de protectie a retelei private de serviciu

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea asigurării interoperabilității livrabilelor componentei de protectie a rețelei private de serviciu, între ele, pentru a permite atât administrarea centralizată a tuturor echipamentelor de tip gateway de protecție de la nivelul aceleiași consolei centrale de management (CM4), cât și activarea și aplicarea simultană a politicilor de securitate, aceleași — respectiv, cu referire la aceleași tipuri de servicii, în topologie de acces și în context de securitate similare — pentru toate componentele de tip gateway (GP1 - GP3), pe baza unui vocabular comun de definire a acestora.

Cerințe generale

Echipamentele de tip Gateway de protecție vor oferi următoarele caracteristici:

- Un nivel de management și control separat de nivelul de procesare a traficului pentru protecția rețelei.
- Nivelul de procesare funcționează prin paralelizarea tuturor mecanismelor de protecție activate.
- Nivelul de control oferă posibilitatea partiționării sistemului și instanțierea mai multor routere virtuale pentru fiecare partiție în parte.

- Posibilitatea configurării fiecarei partiții pentru operare în mod Layer 3 sau Layer 2, inclusiv Layer 2 transparent.
- Posibilitatea configurării porturilor pentru operare în mod TAP, pentru analiza traficului recepționat sau, în mod standard pentru procesarea traficului pe baza politicilor de securitate definite în sistem.
- Posibilitatea definirii politicilor de securitate atât pentru trafic IPv4 cât şi pentru IPv6.
- Posibilitatea procesării traficului pe baza politicilor de securitate chiar şi în situații de rutare asimetrică.
- Posibilitatea definirii politicilor de securitate pentru trafic identificat prin 802.1q sau pentru trafic pentru care se identifică aplicația folosită pentru generarea traficului.
- Suport pentru cel puțin 5000 de profile de aplicații ce vor putea fi utilizate pentru definirea şi aplicarea politicilor de securitate.
- Posibilitatea identificării utilizatorului şi a terminalului folosit prin integrarea cu sistemele de management existente (Microsoft Active Directory sau LDAP) şi corelarea cu adresa IP alocată utilizatorului.
- Posibilitatea identificării conținutului de date pentru sesiunile de tip SSL prin intermedierea stabilirii sesiunilor desemnate pe baza politicilor de securitate aplicabile.
- Suport pentru politici de tip NAT atât pentru adresa IP sursă cât şi pentru adresa IP destinație.
- Mecanisme integrate de protectie împotriva atacurilor de tip DoS bazate pe utilizarea de pachete de date fragmentate.
- Suport pentru definirea politicilor de management de tip QoS.
- Posibilitatea de auditare la nivel de sesiune prin înregistrarea tuturor parametrilor necesari din cadrul pachetelor IP.
- Posibilitatea de raportare pe baza aplicațiilor folosite sau a traficului şi a factorilor de risc de securitate asociați tipului de trafic.
- Posibilitatea definirii de politici pentru exportarea automată a rapoartelor prin trimiterea pe e-mail.
- Posibilitatea exportării rapoartelor în format csv sau pdf.
- Echipamentele de tip gateway de protecție vor asigura susținerea traficului pentru cel puțin 1,000 de utilizatori pentru serviciul de VPN (cu suport SSL, IPSec şi IKE/XAUTH).
- Echipamentele de tip gateway de protecție vor implementa cel puțin o interfață fizică de rețea dedicată, pentru acces administrativ out-of-band.

- Echipamentele de tip gateway de protecție vor implementa cel puțin o interfață fizică de management dedicată, pentru funcțiile de HA.

Dimensionarea specifică a Componentei de protectie a rețelei private de serviciu este dată la pct. 3.3.19-22, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.11. Componenta de retenție a datelor de audit

Context și rol

Componenta (cod C-XI) asigură colectarea, agregarea și valorificarea analitică și operațională a informației martor de audit tehnic ("loguri", și informație asimilată), pentru întreaga infrastructură, precum și informația de audit specific pentru autorizarea accesului terminalelor autorizate la serviciile platformei și jurnalizarea utilizării resurselor acestia.

Componenta de retenție a datelor de audit este alcatuită din următoarele tipuri de livrabile:

- Senzor de audit general (cod SA);
  Instanțe pentru colectarea și consolidarea informației martor de audit ("log forwarder").
- Consola de management de Tip 5 (cod CM5).
  Consola centrală de management, indexare și valorificare date martor de audit.
- Echipamente de stocare de Tip 2 (cod ES2);
  Suport hardware distribuit, la nivel central, pentru retenția datelor martor de audit.

Diagrama de mai jos introduce livrabilele componentei de retenție a datelor de audit și poziționarea acestora în arhitectura platformei.

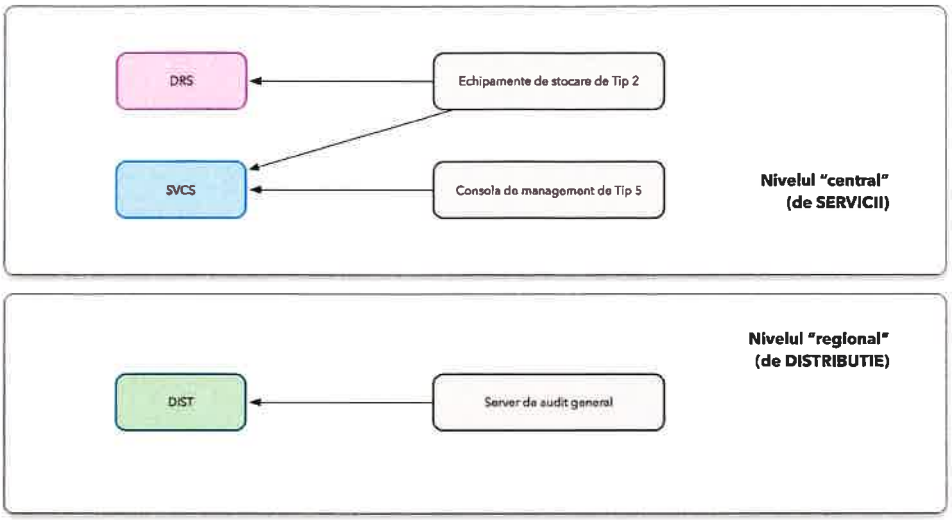

Diagrama (14) — Componenta de retenție a datelor de audit

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea asigurării suportului pentru toate echipamentele (legătura cu C-I — C-X), precum și pentru instanțele active de servicii și pentru cele de management, generatoare de informație martor de audit (de tip "log", sau asimilată), pentru a oferi suport operațional specific în sensul valorificării acestora.

Cerințe generale

Prin Serverele de audit și Consola de management de tip 5 se vor asigura următoarele:

- Soluția va asigura managementul datelor de audit generate de echipamente și de instanțele active de servicii, inclusiv a celor implementate în medii virtuale;
- Platforma va asigura consolidarea și valorificarea datelor martor de audit, cu acoperire și vizibilitate completă asupra întregii platforme, pentru toate punctele din rețea, și va permite managementul datelor de audit pentru întreaga infrastructură;
- Soluția va permite instalarea în topologie multiplu-redundantă, de tip cluster activ-activ și activ-pasiv;
- Soluția trebuie să asigure următoarele capabilități și funcționalități:
    - Va colecta, analiza și corela date de la toate sistemele, aplicațiile și serviciile din infrastructură, fără a se baza pe sisteme externe suport de tip de bază de date;

- Va permite importul datelor din sisteme de baze de date relaționale, cu suport cel putin pentru: Microsoft SQL Server, Oracle Database, MySQL, PostgreSQL;
- Va permite agregarea datelor din fișiere sistem, jurnale de audit specifice, precum și comunicație directă de tip syslog (peste rețea, prin porturi TCP/UDP configurabile), cel puțin pentru sisteme de operare, echipamente hardware, aplicații, servicii sistem și instanțe API.

- Căutarea datelor relevante, pentru analiza informațiilor de audit se va face pe baza de scheme de cautare (parametrii de cautare agregați) ce va putea fi construită în timp real, la momentul executarii căutării, și va putea fi rulată inclusiv asupra datelor ce sunt colectate în timp real;
- Soluția trebuie să permită atât căutarea în timp real asupra datelor de audit colectate, cât și afisarea rezultatelor în context istoric asupra aceluiași set de date analizate;
- Soluția trebuie să permită agregarea, corelarea și căutarea în colecții de evenimente din (respectiv generate de) sisteme și aplicații diferite, relativ la o aceeași tranzactie sau la un același set de tranzacții;
- Soluția trebuie să permită afișarea interactivă a rezultatelor căutării datelor de audit, cu posibilitatea de a mări/micșora în timp real perioada de timp de referință, pentru datele analizate, în scopul de a identifica tendințe, vârfuri de sarcină și anomalii;
- Soluția trebuie să ofere posibilitatea de eșantionare a seturilor de date de audit, astfel încât să permită regasirea și analiza rapidă a datelor relevante pentru termenii de căutare folosiți;
- Soluția trebuie să permită adnotarea evenimentelor de audit pentru a adauga context suplimentar de corelare;
- Soluția trebuie să permită detecția modelelor de corelare și de valorificare relevante indiferent de sursa si de tipul datelor de audit;
- Soluția va permite personalizarea tabloului de bord și va permite generarea, exportul și distribuția de rapoarte personalizate, cel puțin în format PDF;
- Soluția va permite definirea de alerte, cel puțin pentru evenimentele de audit critice, care vor putea declanșa acțiuni sau seturi de acțiuni de alertare a administratorilor;
- Soluția va permite integrarea nativă cu aplicații terțe prin API ce poate exporta întregul set de functionalități, respectiv prin acces direct la nivel de date prin conexiune de tip ODBC;
- Soluția va permite integrarea nativă cu sisteme de tip Hadoop, oferind mecanisme integrate de transfer bi-direcțional (import/export) și de cautare în seturile de date de audit;

- Soluția va oferi mecanisme integrate de acces la instrumentele de administrare și de exploatare a funcționalităților componentei, precum și de securizare a accesului autorizat prin HTTPS (TLS) și SSH;
- Soluția va oferi mecanisme integrate, configurabile, de anonimizare și de mascare a datelor confidențiale din afișarea rezultatelor de căutare asupra seturilor de date de audit;
- Soluția va oferi mecanisme automatizate de amprentare criptografică a datelor de audit indexate, respectiv va permite semnarea evenimentelor individuale și a seturilor de evenimente corelate, astfel încât se va putea garanta integritatea respectivelor seturi de date.

La nivelul Echipamentelor de stocare de Tip 2 se vor asigura următoarele:

- Suport de acces la date pe bază de protocoale standard uzuale și interfețele programabile specifice, inclusiv pentru S3, Swift, NFS și HDFS;
- Suport funcțional multiprotocol nativ, pe aceeași platformă, fără componente intermediare de tip gateway;
- Management integrat pentru întreaga arhitectură și pentru toate serviciile oferite, fără limitări în ceea ce privește numărul de utilizatori sau de aplicații care pot accesa platforma;
- Arhitectură nativă distribuită multi-nod si multi-site, activ-activ, cu spatiu de adresare global unificat;
- Capacitatea de stocare utilă solicitată va fi accesibilă pentru citire și scriere din toate punctele de prezență acoperite;
- Functionalități integrate de management și de protecție a datelor, inclusiv prin utilizarea transparentă a metodelor criptografice;
- Funcționalități incluse, în configurația oferită, de asigurare a scalabilității și de redistribuire activă a sarcinii între noduri, la nivel de site;
- Mirroring local și replicare globală, multi-site, a datelor, cu funcționalități mature pentru realizarea coerenței globale și suport pentru versionarea datele stocate;
- Politici aplicabile accesului și gestionaării ciclului de viață (retenție) a datelor.

Dimensionarea specifică a Componentei de retenție a datelor de audit este dată la pct. 3.3.23-24 și 3.3.29, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.2.12. Componenta de infrastructură fizică suport

Context și rol

Componenta (C-XII) asigură componentele și reperele pentru suportul fizic de poziționare, de susținere și de protecție a echipamentelor, respectiv la locul de instalare și funcționare a acestora, inclusiv protecția alimentării cu energie electrică și protecția împotriva accesului fizic neautorizat.

Componenta de infrastructură fizică suport este alcatuită din următoarele tipuri de livrabile:

- Infrastructură fizică suport (cod IFS).
  Componentele, de tip rack de palier și repere asociate, de montare și susținere a echipamentelor (cel puțin R1A, R1B și SW1A) la nivel de școală.

Diagrama de mai jos introduce livrabilele componentei de infrastructură fizică suport și poziționarea acestora în arhitectura platformei:

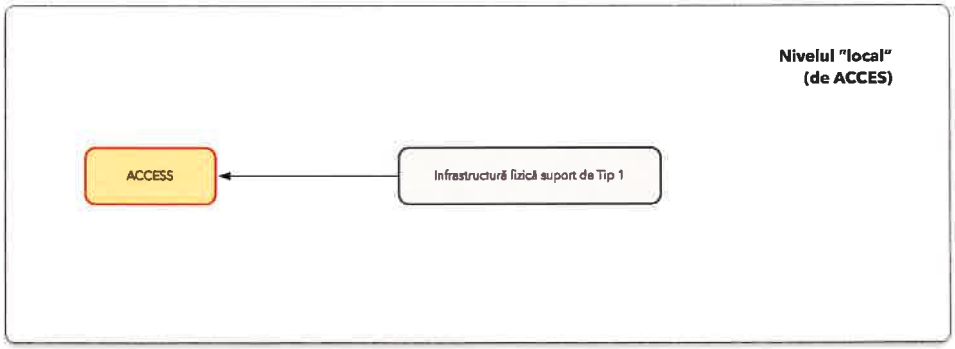

Diagrama (15) — Componenta de infrastructură fizică suport

Pentru asigurarea viabilității operaționale a platformei trebuie avute în vedere cel puțin următoarele:

- Necesitatea asigurării, de către infrastructura fizică suport, a condițiilor optime de instalare a echipamentelor și a reperelor din nivelul de acces (inclusiv acomodarea dimensiunilor și a greutății), susținere fizică a acestora, asigurarea condițiilor optime de interconectare, de răcire, pentru protecția alimentării și controlul accesului fizic la acestea (legătura cu C-I, livrabilele Router de Tip 1A și 1B din C-II, livrabilele Switch de Tip 1A și 1B din C-III).

Cerințe generale

Dimensionarea specifică a Componentei de infrastructură fizică suport este dată la pct. 3.3.30, unde sunt prezentate specificațiile tehnice pentru livrabilele corespunzătoare și configurația respectiv necesară pentru atingerea obiectivelor proiectului.

3.3. Specificații tehnice și dimensionare

3.3.1. Echipamente de tip AP Wi-Fi

Dimensionarea soluției

Echipamente de acces primar Wi-Fi (Echipamente de tip AP Wi-Fi, parte a Componenta de acces primar în tehnologie Wi-Fi — codificare livrabil APW/C-I)

- 20000 seturi APW/C-I (1 echipament de tip AP Wi-Fi, în fiecare set)

Specificații tehnice și configurație

Pentru livrabilele APW/C-I, fiecare echipament de tip AP Wi-Fi va fi echipat, configurat și licențiat (dacă soluția presupune licențiere pentru activarea funcționalităților, a capacității și/sau a performanței solicitate) pentru a asigura cel puțin:

- 2 interfețe radio;
- 4x4 MU-MIMO, minim 3 fluxuri spațiale și lărgime de bandă disponibilă de până la cel puțin 80 MHz pe canal;
- antene omnidirecționale integrate, pentru frecvențele de 2,4GHz si 5 GHz, cu un câștig minim de 4 dBi;
- 2 interfețe Gigabit Ethernet 100/1000Base-T, cu suport pentru agregare 802.3ad LACP și 802.3at.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea echipamentelor în diferite situații (prindere pe tavan, perete, sau pe cutii de conectorizare), inclusiv pentru pentru interconectarea în mediul local LAN și racordarea la sistemul de alimentare cu energie electrică (via cablu de rețea și funcționalitatea PoE+ oferită de livrabilele de tip SW1A sau, după caz, SW1B).

Configurația va include, fără costuri suplimentare pentru beneficiar pe durata normală de viață a soluției (respectiv pentru minim 5 ani), cel puțin:

- Protecția acestuia (în conformitate cu legislația aplicabilă) împotriva defecțiunilor generate de vicii de material și de fabricație pentru hardware;
- Dreptul neexclusiv de utilizare software, inclusiv pentru componentele funcționale integrate (embedded software/firmware, acolo unde este cazul);
- Accesul la sursele de pachete corective software (hotfix/patch) funcționale și de securitate, la informația necesară pentru aplicarea acestora, precum și la resursele necesare pentru soluționarea problemelor tehnice identificare.

Echipamentele care prezintă defecțiuni generate de vicii de material și de fabricație vor fi înlocuite fără costuri suplimentare, în cel mult 2 zile lucrătoare de la notificarea defecțiunii, pentru echipamentele din nivelul de distribuție și de servicii, respectiv în cel mult 4 zile lucrătoare, pentru cele din nivelul de acces, fără a fi necesară returnarea prealabilă a acestora către producător.

Beneficiarul va avea acces fără costuri suplimentare, pe baza unui program zilnic de tip 8/5, în zilele de lucru, la sursele de pachete corective și la resursele necesare pentru implementarea acestora și pentru soluționarea problemelor tehnice identificate.

În urma înlocuirii echipamentelor care prezintă defecțiuni generate de vicii de material și de fabricație, precum și în cazul aplicării de pachete corective software, platforma va fi repusă în starea normală de funcționare, fără costuri suplimentare pentru beneficiar.

3.3.2. Router de Tip 1A

Dimensionarea soluției

Gateway WAN de Acces (Router de Tip 1A, parte a Componentei de dirijare a traficului și de interconectare WAN — codificare livrabil R1A/C-II)

- 1000 seturi R1A/C-II (1 echipament de tip router, în fiecare set)

Specificații tehnice și configurație

Pentru livrabilele R1A/C-II, fiecare echipament de tip router va fi echipat, configurat și licențiat (dacă soluția presupune licențiere pentru activarea funcționalităților, a capacității și/sau a performanței solicitate) pentru a asigura cel puțin:

- cel putin 2 interfețe 1Gbps Ethernet cu conector RJ45, din care cel putin una sa poată fi echipată si un conector optic de tip SFP și posibilitatea de a adauga in viitor 2 interfete 1 Gigabit Ethernet cu conector RJ45;

- toate licențele software incluse pentru asigurarea functionalitatilor cerute și a performanței specifice (throughput cu criptare pentru trafic de tip IMIX, inclusiv overhead) de 100Mbps in conditiile descrise.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

Configurația va include, fără costuri suplimentare pentru beneficiar pe durata normală de viață a soluției (respectiv pentru minim 5 ani), cel puțin:

- Protecția acestuia (în conformitate cu legislația aplicabilă) împotriva defecțiunilor generate de vicii de material și de fabricație pentru hardware;
- Dreptul neexclusiv de utilizare software, inclusiv pentru componentele funcționale integrate (embedded software/firmware, acolo unde este cazul);
- Accesul la sursele de pachete corective software (hotfix/patch) funcționale și de securitate, la informația necesară pentru aplicarea acestora, precum și la resursele necesare pentru soluționarea problemelor tehnice identificare.

Echipamentele care prezintă defecțiuni generate de vicii de material și de fabricație vor fi înlocuite fără costuri suplimentare, în cel mult 2 zile lucrătoare de la notificarea defecțiunii, pentru echipamentele din nivelul de distribuție și de servicii, respectiv în cel mult 4 zile lucrătoare, pentru cele din nivelul de acces, fără a fi necesară returnarea prealabilă a acestora către producător.

Beneficiarul va avea acces fără costuri suplimentare, pe baza unui program zilnic de tip 8/5, în zilele de lucru, la sursele de pachete corective și la resursele necesare pentru implementarea acestora și pentru soluționarea problemelor tehnice identificate.

În urma înlocuirii echipamentelor care prezintă defecțiuni generate de vicii de material și de fabricație, precum și în cazul aplicării de pachete corective software, platforma va fi repusă în starea normală de funcționare, fără costuri suplimentare pentru beneficiar.

3.3.3. Router de Tip 1B

Dimensionarea soluției

Gateway WAN de Acces (Router de Tip 1B, parte a Componentei de dirijare a traficului și de interconectare WAN — codificare livrabil R1B/C-II)

- 3500 seturi R1B/C-II (1 echipament de tip router, în fiecare set)

Specificații tehnice și configurație

Pentru livrabilele R1B/C-II, fiecare echipament de tip router va fi echipat, configurat și licențiat (dacă soluția presupune licențiere pentru activarea funcționalităților, a capacității și/sau a performanței solicitate) pentru a asigura cel puțin:

- cel putin 2 interfețe 1Gbps Ethernet cu conector RJ45, din care cel putin una sa poată fi echipată si un conector optic de tip SFP;
- toate licențele software incluse pentru asigurarea functionalitatilor cerute și a performanței specifice (throughput cu criptare pentru trafic de tip IMIX, inclusiv overhead) de 50Mbps in conditiile descrise.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

Configurația va include, fără costuri suplimentare pentru beneficiar pe durata normală de viață a soluției (respectiv pentru minim 5 ani), cel puțin:

- Protecția acestuia (în conformitate cu legislația aplicabilă) împotriva defecțiunilor generate de vicii de material și de fabricație pentru hardware;
- Dreptul neexclusiv de utilizare software, inclusiv pentru componentele funcționale integrate (embedded software/firmware, acolo unde este cazul);
- Accesul la sursele de pachete corective software (hotfix/patch) funcționale și de securitate, la informația necesară pentru aplicarea acestora, precum și la resursele necesare pentru soluționarea problemelor tehnice identificare.

Echipamentele care prezintă defecțiuni generate de vicii de material și de fabricație vor fi înlocuite fără costuri suplimentare, în cel mult 2 zile lucrătoare de la notificarea defecțiunii, pentru echipamentele din nivelul de distribuție și de servicii, respectiv în cel mult 4 zile lucrătoare, pentru cele din nivelul de acces, fără a fi necesară returnarea prealabilă a acestora către producător.

Beneficiarul va avea acces fără costuri suplimentare, pe baza unui program zilnic de tip 8/5, în zilele de lucru, la sursele de pachete corective și la resursele necesare pentru implementarea acestora și pentru soluționarea problemelor tehnice identificate.

În urma înlocuirii echipamentelor care prezintă defecțiuni generate de vicii de material și de fabricație, precum și în cazul aplicării de pachete corective software, platforma va fi repusă în starea normală de funcționare, fără costuri suplimentare pentru beneficiar.

3.3.4. Router de Tip 2

Dimensionarea soluției

Gateway WAN de Distribuție (Router de Tip 2, parte a Componentei de dirijare a traficului și de interconectare WAN — codificare livrabil R2/C-II)

- 1 set R2/C-II (cel puțin 8 echipamente de tip router, în fiecare set)

Specificații tehnice și configurație

Pentru livrabilele R2/C-II, fiecare echipament de tip router va fi echipat, configurat și licențiat (dacă soluția presupune licențiere pentru activarea funcționalităților, a capacității și/sau a performanței solicitate) pentru a asigura cel puțin:

- 4 porturi SFP Gigabit Ethernet dintre care doua populate cu SFP-uri 1000Base-T;
- 2 porturi 10 Gigabit Ethernet populate cu 2 SFP-uri 10Gigabit Ethernet pentru fibra optica multimode cu o lungime de pana la 300m;
- capacitate total de procesare specifică (throughput) de 20 Gbps;
- capacitate de criptare de 8 Gbps, cu suport pentru criptare de ultima generatie (cel putin AES256);
- 1.000.000 rute IPv4;
- 4000 tunele IPSEC;
- 4000 tunele GRE;
- să implementeze suita de protocoale MPLS L3VPN;
- să implementeze protocoalele de rutare: BGP, OSPF, IS-IS, RIP, OSPFv3, RIPng;
- un slot de extensie liber pentru extinderi viitoare.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

Configurația va include, fără costuri suplimentare pentru beneficiar pe durata normală de viață a soluției (respectiv pentru minim 5 ani), cel puțin:

- Protecția acestuia (în conformitate cu legislația aplicabilă) împotriva defecțiunilor generate de vicii de material și de fabricație pentru hardware;
- Dreptul neexclusiv de utilizare software, inclusiv pentru componentele funcționale integrate (embedded software/firmware, acolo unde este cazul);

- Accesul la sursele de pachete corective software (hotfix/patch) funcționale și de securitate, la informația necesară pentru aplicarea acestora, precum și la resursele necesare pentru soluționarea problemelor tehnice identificare.

Echipamentele care prezintă defecțiuni generate de vicii de material și de fabricație vor fi înlocuite fără costuri suplimentare, în cel mult 2 zile lucrătoare de la notificarea defecțiunii, pentru echipamentele din nivelul de distribuție și de servicii, respectiv în cel mult 4 zile lucrătoare, pentru cele din nivelul de acces, fără a fi necesară returnarea prealabilă a acestora către producător.

Beneficiarul va avea acces fără costuri suplimentare, pe baza unui program zilnic de tip 8/5, în zilele de lucru, la sursele de pachete corective și la resursele necesare pentru implementarea acestora și pentru soluționarea problemelor tehnice identificate.

În urma înlocuirii echipamentelor care prezintă defecțiuni generate de vicii de material și de fabricație, precum și în cazul aplicării de pachete corective software, platforma va fi repusă în starea normală de funcționare, fără costuri suplimentare pentru beneficiar.

3.3.5. Router de Tip 3A

Dimensionarea soluției

Gateway WAN de Servicii (Router de Tip 3A, parte a Componentei de dirijare a traficului și de interconectare WAN — codificare livrabil R3A/C-II)

- 1 set R3A/C-II (cel puțin 2 echipamente modulare de tip router, în fiecare set)

Specificații tehnice și configurație

Pentru livrabilele R3A/C-II, fiecare echipament de tip router va fi echipat, configurat și licențiat (dacă soluția presupune licențiere pentru activarea funcționalităților, a capacității și/sau a performanței solicitate) pentru a asigura cel puțin:

- 2 milioane de rute IPv4/IPv6;
- Procesor de control redundant si switch-fabric (sau echivalent) redundant;
- Functia de Carrier-Grade NAT pentru minim 45 milioane de sesiuni;
- Implementarea funcționalității de tip Carrier-Grade NAT într-un mod redundant, folosind cel puțin două componente hardware redundante, identic configurate;
- Capacitate de comutare pentru fiecare slot de cel puțin 400 Gbps;
- Capacitate de comutare totală de minim 3Tbps;
- 4 interfețe 40 GE dispuse în cel puțin 2 sloturi diferite.

Vor fi incluse toate reperele şi subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum şi pentru interconectarea în mediile LAN.

Configuraţia va include, fără costuri suplimentare pentru beneficiar pe durata normală de viaţă a soluţiei (respectiv pentru minim 5 ani), cel puţin:

- Protecţia acestuia (în conformitate cu legislaţia aplicabilă) împotriva defecţiunilor generate de vicii de material şi de fabricaţie pentru hardware;
- Dreptul neexclusiv de utilizare software, inclusiv pentru componentele funcţionale integrate (embedded software/firmware, acolo unde este cazul);
- Accesul la sursele de pachete corective software (hotfix/patch) funcţionale şi de securitate, la informaţia necesară pentru aplicarea acestora, precum şi la resursele necesare pentru soluţionarea problemelor tehnice identificare.

Echipamentele care prezintă defecţiuni generate de vicii de material şi de fabricaţie vor fi înlocuite fără costuri suplimentare, în cel mult 2 zile lucrătoare de la notificarea defecţiunii, pentru echipamentele din nivelul de distribuţie şi de servicii, respectiv în cel mult 4 zile lucrătoare, pentru cele din nivelul de acces, fără a fi necesară returnarea prealabilă a acestora către producător.

Beneficiarul va avea acces fără costuri suplimentare, pe baza unui program zilnic de tip 8/5, în zilele de lucru, la sursele de pachete corective şi la resursele necesare pentru implementarea acestora şi pentru soluţionarea problemelor tehnice identificate.

În urma înlocuirii echipamentelor care prezintă defecţiuni generate de vicii de material şi de fabricaţie, precum şi în cazul aplicării de pachete corective software, platforma va fi repusă în starea normală de funcţionare, fără costuri suplimentare pentru beneficiar.

3.3.6. Router de Tip 3B

Dimensionarea soluţiei

Gateway WAN de DRS (Router Tip 3B, parte a Componentei de dirijare a traficului şi de interconectare WAN — codificare livrabil R3B/C-II)

- 1 set R3B/C-II (cel puţin 1 echipament de tip router, în fiecare set)

Specificații tehnice și configurație

Pentru livrabilele R3B/C-II, fiecare echipament de tip router va fi echipat, configurat și licențiat (dacă soluția presupune licențiere pentru activarea funcționalităților, a capacității și/sau a performanței solicitate) pentru a asigura cel puțin:

- 2 milioane de rute IPv4/IPv6;
- Capacitate de comutare pentru fiecare slot de cel puțin 400 Gbps;
- Capacitate de comutare totala de minim 3Tbps;
- 2 interfețe 40 GE.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

Configurația va include, fără costuri suplimentare pentru beneficiar pe durata normală de viață a soluției (respectiv pentru minim 5 ani), cel puțin:

- Protecția acestuia (în conformitate cu legislația aplicabilă) împotriva defecțiunilor generate de vicii de material și de fabricație pentru hardware;
- Dreptul neexclusiv de utilizare software, inclusiv pentru componentele funcționale integrate (embedded software/firmware, acolo unde este cazul);
- Accesul la sursele de pachete corective software (hotfix/patch) funcționale și de securitate, la informația necesară pentru aplicarea acestora, precum și la resursele necesare pentru soluționarea problemelor tehnice identificare.

Echipamentele care prezintă defecțiuni generate de vicii de material și de fabricație vor fi înlocuite fără costuri suplimentare, în cel mult 2 zile lucrătoare de la notificarea defecțiunii, pentru echipamentele din nivelul de distribuție și de servicii, respectiv în cel mult 4 zile lucrătoare, pentru cele din nivelul de acces, fără a fi necesară returnarea prealabilă a acestora către producător.

Beneficiarul va avea acces fără costuri suplimentare, pe baza unui program zilnic de tip 8/5, în zilele de lucru, la sursele de pachete corective și la resursele necesare pentru implementarea acestora și pentru soluționarea problemelor tehnice identificate.

În urma înlocuirii echipamentelor care prezintă defecțiuni generate de vicii de material și de fabricație, precum și în cazul aplicării de pachete corective software, platforma va fi repusă în starea normală de funcționare, fără costuri suplimentare pentru beneficiar.