Combridge Deutsche Telekom Group

ANEXA NR. 1. SPEFICAȚII TEHNICE ALE PRODUSELOR ȘI SERVICIILOR COMBRIDGE

1. Descriere Generală

CPE-A (Smart CPE Advance) – echipament dotat cu 3G backup, Gestionare echipament în Cloud, 4x Gigabit Ethernet LAN
IACC (Combridge Internet Access) – Acces Internet furnizat de Combridge pe fibră optică; 100 Mbps; adresă IP Publică
VPN (Virtual Private Network) – Conectarea locațiilor prin rețele private virtuale (VPN)
CCS (Corporate Communication Solution) – Soluție corporativă de comunicare IP PBX; Firewall; DDoS; Filtrare conținut; Fax2Mail/Mail2Fax; Hosting; server de Mail
CCS-E – Corporate Communication Solution Entry pana la 20 utilizatori
CCS-A – Corporate Communication Solution Advanced pentru un număr nelimitat de utilizatori
VPS-E (Virtual Private Server Easy) – Server Privat Virtual "Easy"
VPS-A (Virtual Private Server Advanced) – Server Privat Virtual "Advanced"
VPS-S (Virtual Private Server Star) – Server Privat Virtual "Star"
MLAN/MWLAN – Gestionare rețea locală prin fir sau wireless.
VHB/M/HE/EX – voice headsets basic/medium/high end/executive sunt telefoane IP de nivel elementar (B), mediu (M), top (HE), secretariat (EX).
LBA, LPL; LPR – platformă de WiFi marketing Linkyfi basic (LBA), Plus (LPL) și Pro (LPR).
MWL-CMBW-ANM și MWL-CMBW-RNM – platformă de administrare rețea

Procesul de comandă este unul simplu, se pleacă de la Cloud (Smart CPE) și se adaugă funcționalități conform necesităților companiei, așa cum puteți observa în Fig. 1.

Adaugă valoare

Servicii				Beneficii adăugate
Smart CPE-A	VPN	CCS-A/E	MLAN/MWLAN*	Managed LAN/WLAN
Smart CPE-A	VPN	CCS-A/E	VHHE*+VHEX*	Modul de extensie pentru secretariat
			VHHE*	Telefon IP cu Port Gigabit și Bluetooth
			VHM*	Telefon IP cu Port Gigabit
			VHB*	Telefon IP
Smart CPE-A	VPN	CCS-A/E	VPS-S	Putere de procesare VPS Star
			VPS-A	Putere de procesare VPS Advanced
			VPS-E	Putere de procesare VPS Easy
Smart CPE-A	VPN	CCS-A		IP PBX; Firewall; DDoS; Filtrare de conținut; Hosting; Fax2Mail/Mail2Fax; server de Mail; utilizatori nelimitați
		CCS-E		IP PBX; Firewall; DDoS; Filtrare de conținut; Hosting; Fax2Mail/Mail2Fax; Mail server; up to 20 users
Smart CPE-A	VPN			Asigură o rețea virtuală privată (VPN) între locații
Smart CPE-A				Advanced: backup 4G; Gestionare echipament în Cloud; 802.11 b/g/n; 4 porturi Gigabit Ethernet LAN

Fig. 1.

*Coduri de comandă:
Managed LAN: MLAN-8P-SEL-1YR/3YR, MLAN-24P-E-SEL-1YR/3YR, MLAN-24P-A-SEL-1YR/3YR, MLAN-48P-SEL-1YR/3YR, MLAN-8P-CON-1YR/3YR, MLAN-24P-E-CON-1YR/3YR, MLAN-24P-A-CON-1YR/3YR, MLAN-48P-CON-1YR/3YR
Managed WLAN: MWL-122-CON-1YR, MWL-130-CON-1YR/3YR, MWL-230-CON-1YR/3YR, MWL-245-CON-1YR/3YR, MWL-250-CON-1YR/3YR, MWL-550-CON-1YR/3YR, MWL-1130-CON-1YR/3YR, MWL-122-SEL-1YR, MWL-130-SEL-1YR/3YR, MWL-230-SEL-1YR/3YR, MWL-245-SEL-1YR/3YR, MWL-250-SEL-1YR/3YR, MWL-550-SEL-1YR/3YR, MWL-1130-SEL-1YR/3YR

Serviciile sus menționate sunt detaliate în capitolele următoare.

2. Smart CPE Advanced (CPE-A)

Smart CPE Advanced (CPE-A):

- 3G Backup: Da
- Trafic nelimitat
- LAN: 5xGigaEth
- PoE: 2 porturi
- Wlan: 802.11a/b/g/n

Echipamentele inteligente Combridge, disponibile atât cu alimentare POE cât și cu opțiuni radio, oferă companiilor mici si mijlocii o soluție completă de VPN cu back-up 3G și posibilitatea de configurare la distanță a echipamentelor. Soluția este una avantajoasă și stabilă atât pentru utilizatorii ce se conectează pe fir cât și pentru cei ce se conectează wireless sau la distanță. Traficul nelimitat atât pe conexiunea principală de Internet cât și pe cea de backup 3G oferă o perspectivă clară a costului operațional lunar.

Avantajele Smart CPE:

- Scalabiliate faţă de modificările de configuraţie şi efort minim necesar pentru reconfigurarea reţelei, în cazul suplimentării locaţiilor de acces din reţeaua clientului.
- Gestionarea punctelor de lucru la distanță
- Management-ul se realizează în cloud, server-ul de cloud este găzduit într-un centru de colocare de tip II, Tier IV SAS 70 cu back-up-uri automate si capabilități de recuperare în caz de dezastru.
- Pune la dispozitie funcționalitatea wireless SSID
- Alocarea eficientă a lăţimii de bandă
- Un singur echipament adecvat atât pentru VPN cât și pentru Internet

Caracteristici:

- **Conectivitate flexibilă si fiabilă**

Prin soluția Combridge, Layer 3 IPsec VPN, punctele de lucru acceseaza cu ușurință și în siguranță intranetul companiei, păstrându-se un control total asupra fluxului de informații. Cu un control al accesului (AC) integrat si posibilitatea de afișare a statisticilor, CPE-A poate lua decizii de forwarding bazate pe identitatea utilizatorului sau a tipului dispozitivului, securizând accesul la intranet dar oferind în același timp conectivitate pentru a vizualiza și configura noi puncte de lucru.

- **Securitate Wi-Fi Enterprise Class**

CPE-A are integrat un modul de analiză spectrală pentru identificarea fluxurilor de date legitime și un sistem de prevenire a intruziunilor (WIPS) fără a fi necesare taxe suplimentare de licențiere. Aceste caracteristici ii oferă administratorului capacitatea de a identifica orice posibilă interferență WiFi, de a realiza planuri de dezvoltare și de a pune la dispoziție sucursalelor un acces stabil și sigur în conformitate cu standardele în vigoare.

- **Comutare securizata la implementarea la cerere**

CPE-A oferă o funcționalitate de comutare robustă, în armonie cu infrastructura Wi-Fi, inclusiv o politică unitară de alocare lățime de bandă, gestionare și raportare. CPE-A poate fi activat prin simpla expediere și conectare a echipamentului la o rețea cu acces la Internet, el va găsi în mod automat sistemul de gestionare a rețelei (NMS) de unde își va descărca configurația, politicile de securitate asociate companiei și va oferi instantaneu servicii dispozitivelor conectate.

- **Securitate extinsă**

Printr-o singură politică unificată se realizează măsuri de securitate și de control al accesului unui utilizator. Astfel se poate controla cum și când un utilizator se poate conecta la Intranet fie prin cablul fie prin wireless asigurându-se securitatea indiferent de modul de conectare.

Pentru activarea Smart CPE este necesară o conexiunea la Internet ce poate fi:

- Acces Internet furnizat de Combridge (IACC)
- Acces internet proprietate client

2.1. Acces internet furnizat de Combridge (IACC)

Rețeaua Combridge acoperă majoritatea marilor orașe din Romania.

Serviciile IP sunt implementate pe rețeaua MPLS a grupului Deutsche Telekom/Magyar Telekom.

Caracteristicii IACC:

- **Soluție FTTB (Fiber to the Building)**
- **IP public**
- **Viteză garantată de transfer 100 Mbps (upload/download)**
- **Utilizare simetrică**
- Latență medie garantată de 0,03ms/km
- Pierdere medie de pachete de sub 0,5%
- Conexiune dedicată cu SLA garantat de 99.5%
- Trafic nelimitat
- Statistici online
- 24/7/365 suport tehnic
- Analize de performanță trimestriale

Termenii şi condiţiile tehnice privind furnizarea serviciilor de Internet furnizate de Combridge

2.1.1. Definire termeni

2.1.1.1. Internet – reprezintă reţeaua mondială de echipamente de comunicaţie publice şi private care sunt interconectate şi folosesc suita de protocoale TCP/IP.

2.1.1.2. Reţeaua COMBRIDGE – reprezintă reţeaua de echipamente de comunicaţie COMBRIDGE (proprietatea COMBRIDGE sau închiriată de COMBRIDGE) care este conectată la Internet printr-unul sau mai multe puncte şi care foloseşte suita de protocoale TCP/IP.

2.1.1.3. Sistemul COMBRIDGE – reprezintă sistemul de comunicaţie al COMBRIDGE, parte a reţelei COMBRIDGE, la care se conectează Beneficiarul, sistem format din: fibră optică, noduri optice, cablu coaxial, amplificatoare RF, cutii de distribuţie, celule radio.

2.1.1.4. Traficul – înseamnă orice transfer de informaţie operat de către Beneficiar în afara reţelei COMBRIDGE şi/sau către Beneficiar din afara reţelei COMBRIDGE şi nu include transferul operat de către Beneficiar în reţeaua furnizorului şi/ sau catre Beneficiar din rețeaua furnizorului.

2.1.1.5. Layer 1, Layer 2 si Layer 3 – se înţeleg nivelele 1, 2, respectiv 3 din modelul de referință ISO OSI (modelul Open Systems Interconnection al International Organization for Standardization).

2.1.1.6. Echipamentul de acces în reteaua COMBRIDGE, denumit în continuare "Echipamentul de acces", se înţelege un echipament conectat direct (Layer 1 sau Layer 2) cu reţeaua COMBRIDGE.

Sub această denumire se includ (fără a se limita la): modemul de cablu, modemul radio, modem de linie închiriată mediaconvertorul de fibră optică, switch aparţinând COMBRIDGE.

2.1.1.7. Interfață conectată Layer 2 cu rețeaua COMBRIDGE, denumită în continuare "interfața direct conectată la reteaua COMBRIDGE ", se numește orice interfață de rețea (placa de rețea de exemplu) a Beneficiarului conectată Layer2 cu un "Echipament de acces". Acestă denumire include (fără a se limita la) echipamente direct conectate în "Echipamentul de acces" sau conectate prin unul sau mai multe echipamente Layer1 sau Layer2 (hub-uri, bridge-uri sau switch-uri). Sub această denumire nu se includ echipamentele Beneficiarului care sunt separate de "Echipamentul de acces" printr-un echipament Layer3 (router de exemplu).

2.1.2. Punerea în funcţiune a serviciului

2.1.2.1. Pentru serviciul de Acces la Internet si comunicatii de date, COMBRIDGE se obligă să instaleze şi să pună în funcțiune serviciul conform datelor de instalare specificate în procesul – verbal de punere în funcțiune a serviciului.

Beneficiarul poate solicita pe durata executării contractului mutarea unei locații la care ii sunt furnizate serviciile, operațiune ale cărei costuri vor fi facturate potrivit ofertei COMBRIDGE în vigoare la data solicitării.

2.1.2.2. Beneficiarul este responsabil:

a) Să desemneze şi să pregătească locaţiile pentru instalarea echipamentelor;

b) Să asigure accesul la corpuri de clădiri interne şi externe pentru amplasarea necesară a sistemului COMBRIDGE, pentru personalul COMBRIDGE implicat în instalarea şi punerea în funcțiune a serviciului;

c) Să faciliteze obţinerea aprobărilor (dacă este cazul), pentru instalarea sistemului COMBRIDGE.

2.1.2.3. Lucrările de punere în funcțiune a serviciului de Acces la Internet si comunicatii de date se consideră a fi încheiate si serviciul se consideră a fi funcțional la data semnării procesului verbal de punere în functiune, sau la data prevăzută în orice alt mijloc de probă direct sau indirect. Dacă Beneficiarul refuză să semneze procesul verbal de punere în funcţiune sau acesta nu poate fi întocmit din orice alte motive, serviciul se consideră pus în funcţiune dacă Beneficiarul nu trimite o notificare scrisă, care să dovedească contrariul, în termen de 24 de ore de la data punerii în funcţiune, conform înregistrărilor interne ale COMBRIDGE, a echipamentului de acces.

2.1.2.4. Pentru instalarea de către COMBRIDGE, în locațiile care fac obiectul contractului, a circuitelor care asigură comunicațiile electronice (circuite ce pot include, cu titlu exemplificativ: cabluri, accesorii, dispozitive de conectică sau alte materiale și activarea serviciului de Acces la Internet si comunicatii de date,

Beneficiarul datorează o taxă de instalare, reprezentând contravaloarea tuturor materialelor utilizate, astfel cum sunt evidențiate în procesul-verbal de punere în funcțiune a serviciului.

Lucrările de instalare, conectare şi configurare a echipamentelor din reţeaua locală (LAN) a Beneficiarului la echipamentul de capăt cad în sarcina exclusivă a Beneficiarului.

2.1.2.5. COMBRIDGE poate asigura, la cererea Beneficiarului, instalarea, conectarea şi configurarea echipamentelor din reţeaua locală a Beneficiarului la echipamentul de capăt. COMBRIDGE va factura către Beneficiar contravaloarea operaţiilor efectuate.

2.1.2.6. Prezentele clauze specifice de Acces la Internet și comunicații de date se completează în mod corespunzător cu clauzele cuprinse în Anexa nr. 1, care sunt aplicabile prin analogie.

2.1.3. Drepturile şi obligaţiile părţilor

2.1.3.1. Prin utilizarea unei capacităţi suficiente, COMBRIDGE va opera continuu reţeaua COMBRIDGE şi conexiunile reţelei COMBRIDGE la Internet. COMBRIDGE garantează Beneficiarului îndeplinirea nevoilor sale de trafic, 365 de zile pe an, 24 de ore pe zi, cu excepţia inoperabilităţii conexiunii internaţionale din cauze independente de COMBRIDGE (de exemplu inoperabilitatea satelitului de telecomunicaţii, a reţelelor terestre naţionale şi internaţionale care asigură accesul la reţeaua Internet), inoperabilitatea reţelei electrice (furnizorul de energie electrică) sau oricare alt terţ cu care COMBRIDGE se află sub contract.

2.1.3.2. COMBRIDGE nu va restricţiona accesul Beneficiarului la nici o destinaţie aflată în Internet. COMBRIDGE sau alţi furnizori pot restricţiona uneori accesul la anumite destinaţii din motive de securitate sau protecţie a reţelelor şi Beneficiarul înţelege ca COMBRIDGE nu este responsabil pentru asemenea acţiuni.

2.1.3.3. COMBRIDGE va asigura back-up şi pentru infrastructura internaţională în măsura posibilităţilor de colaborare cu alţi Furnizori de Servicii Internet locali, sau prin mijloace proprii.

2.1.3.4. Este responsabilitatea COMBRIDGE să asigure repararea echipamentelor COMBRIDGE aflate în operare, în cadrul reţelei COMBRIDGE, dacă defecţiunea echipamentului nu s-a produs din vina Beneficiarului sau a altei persoane pentru care COMBRIDGE nu este răspunzator. Daca acest lucru nu este posibil, echipamentul va fi înlocuit.

2.1.3.5. Beneficiarul înţelege că singurul beneficiar al licenţelor şi drepturilor referitoare la operarea Sistemului COMBRIDGE este COMBRIDGE şi că aceste licenţe şi drepturi sunt exclusiv asociate cu Sistemul COMBRIDGE.

2.1.3.6. Sistemul COMBRIDGE poate fi reamplasat doar de către COMBRIDGE.

2.1.3.7. Beneficiarul nu va sechestra, demonta sau scoate din funcţiune orice echipament aparţinând COMBRIDGE.

2.1.3.8. În cazul în care Beneficiarul doreşte să furnizeze către terţi servicii care fac obiectul prezentului contract, Beneficiarul se obligă să ceară acordul scris al COMBRIDGE, înainte de începerea colaborării cu terţii. Aceasta prevedere este valabilă indiferent dacă distribuirea serviciilor către terţi se face prin sistemul COMBRIDGE sau prin altă infrastructură.

2.1.3.9. COMBRIDGE se obligă să asigure supervizarea continuă a serviciului şi supervizarea periodică (verificări, inspecţii, etc) a sistemului. Pentru a facilita realizarea acestei obligaţii şi în baza unei notificări prealabile trimise de COMBRIDGE, Beneficiarul va permite accesul tehnicienilor COMBRIDGE la sistemul de transmisii de date, astfel încât aceştia să realizeze supervizarea tehnică şi să verifice că echipamentul lucrează în mod corespunzător.

2.1.3.10. Beneficiarul se obligă să nu utilizeze în afara sistemului, să nu copieze şi să nu dezvăluie terţilor nicio aplicaţie software şi/sau know-how implementate de COMBRIDGE. Beneficiarul va fi responsabil pentru toate daunele şi reclamaţiile rezultate din încălcarea acestei prevederi.

2.1.3.11. Beneficiarul se obligă să respecte prevederile Secțiunii 2.1.5.

In cazul în care Beneficiarul încalcă prevederile Secțiunii 2.1.5, COMBRIDGE poate suspenda, pe perioada nedeterminată, fără notificare prealabilă, total sau parțial, serviciile oferite Beneficiarului, până la clarificarea de către părţi a situației care a dus la această suspendare și numai după furnizarea în scris de către Beneficiar de explicații. În acelaşi timp, COMBRIDGE va întrerupe, temporar sau permanent, transmiterea prin reţeaua COMBRIDGE sau stocarea informaţiei furnizate sau primite de către Beneficiar, în special prin eliminarea informaţiei sau blocarea accesului la aceasta, accesul la o reţea de comunicaţii sau prestarea oricărui alt serviciu al societăţii informaţionale, dacă aceste măsuri au fost dispuse de o autoritate publică (potrivit dispoziţiilor legale).

2.1.3.12. COMBRIDGE va respecta confidenţialitatea datelor Beneficiarului transferate prin reţeaua COMBRIDGE. COMBRIDGE are dreptul să şteargă orice informaţie introdusă de Beneficiar în reţeaua COMBRIDGE, care ar putea afecta buna funcţionare a acesteia sau ar putea conduce la întreruperea funcţionării reţelei COMBRIDGE.

2.1.4. Securitate. Beneficiarul se obligă să asigure securitatea reţelei, calculatoarelor şi altor componente ale reţelei sale. COMBRIDGE nu îşi asumă responsabilitatea în cazul apariţiei oricăror probleme de securitate în reţeaua Beneficiarului, obligaţia de a-şi asigura securitatea reţelei aparţinând în exclusivitate Beneficiarului

2.1.4.1. Beneficiarul declară că este de acord să primească, din partea COMBRIDGE, informaţii legate de serviciul primit de la COMBRIDGE, alte servicii oferite de către COMBRIDGE, precum şi orice alte comunicări comerciale prin poştă electronică, poştă, fax sau orice altă modalitate considerată potrivită de către Furnizor.

2.1.4.2. Beneficiarul se obligă să ceară de la COMBRIDGE în scris orice informaţii legate de serviciul contractat numai prin reprezentanţii săi autorizaţi. Dacă aceste cereri vor fi formulate de către alte persoane, care nu sunt autorizate, COMBRIDGE va prelua aceste solicitări, le va transmite către reprezentanţii autorizaţi ai Beneficiarului şi va trimite răspunsul la cerere numai după ce una din persoanele autorizate confirmă în scris validitatea cererii.

2.1.5. Reguli de utilizare a serviciilor COMBRIDGE

2.1.5.1. Aceaste reguli de utilizare a rețelei și serviciilor COMBRIDGE sunt valabile pentru toţi clienţii COMBRIDGE sau terţii care folosesc rețeaua COMBRIDGE ca mediu de comunicare. COMBRIDGE nu tolerează nici un abuz direct sau indirect prin folosirea rețelei sale chiar daca este originat de la clienții (Beneficiarii) COMBRIDGE, de la clienții clienților COMBRIDGE sau orice terți ce folosesc rețeaua COMBRIDGE ca mediu de comunicare.

2.1.5.2. COMBRIDGE consideră ca eliminarea SPAM-ului și a abuzurilor vor rezulta într-un Internet mai ieftin, mai bun și mai eficient pentru clienții săi.

2.1.5.3. COMBRIDGE definește ca abuz sau folosire ilegala a rețelei:

Orice e-mail comercial (comunicare comercială prin intermediul poştei electronice) ce este trimis către o adresă ce nu a cerut și confirmat în mod expres dorinţa de a primi astfel de mesaje. E-mail-urile comerciale includ și nu se limitează la: reclame, sondaje de opinie, oferte promoționale etc. Aceste tipuri de mesaje sunt denumite “Unsolicited BroadcastEmail”/ ”Unsolicited Commercial Email” și vor fi referite în continuare ca SPAM.

Generarea unui trafic neobișnuit de mare cu scopul de a supraîncarca conexiunea unui server sau a unui utilizator internet, sau pentru a epuiza resursele serverelor blocând access-ul utilizatorilor legitimi. Acest tip de abuz va fi definit în continuare ca „flood”.

2.1.5.4. Orice activitate ce are ca scop accesul, obţinerea şi/sau modificarea de informaţii/resurse ce nu au un caracter public. Aceste tipuri de activități includ, fără a se limita la acestea: exploatarea breșelor de securitate pe alte calculatoare conectate la Internet, căutarea (scanarea) după breşe de securitate a unor calculatoare conectate la Internet, folosirea de servicii tip “proxy” fără acordul propietarului acestor servicii.

2.1.5.5. Transmiterea, distribuirea și stocarea de viruși informatici, programe, fișirere sau materiale ce violează legile în vigoare sau sunt protejate prin copyright, mărci de comerț, de fabrică sau de servicii, sau orice alt drept de propietate intelectuală fără autorizațiile necesare, fără a se limita doar la acestea.

2.1.5.6. Trasmiterea, distribuirea și stocarea de materiale obscene, dicriminatorii, rasiste sau care violează legile de control al exportului în vigoare.

2.1.6. Reguli COMBRIDGE

2.1.6.1. Rețeaua COMBRIDGE poate fi folosită de către clienții săi pentru a se conecta la alte rețele, iar utilizatorii rețelei COMBRIDGE înțeleg ca trebuie să se conformeze tuturor regulilor de utilizare a acestor rețele. Clienții (Beneficiarii) COMBRIDGE înțeleg ca COMBRIDGE nu poate avea controlul informației care circulă prin rețeaua COMBRIDGE. Orice supraîncarcare a rețelei COMBRIDGE va fi considerată o folosire neautorizată a rețelei COMBRIDGE și este de aceea interzisă. În mod similar, folosirea de “IP multicast” fără permisiunea COMBRIDGE este interzisă.

2.1.6.2. Clienților care folosesc rețeaua COMBRIDGE, le este interzis și nu au dreptul să permită terților folosirea rețelei COMBRIDGE pentru a trimite SPAM-uri și/sau să utilizeze în mod abuziv serviciul și/sau rețeaua COMBRIDGE sau alte rețele de comunicații electronice. În cazul în care se trimit e-mail-uri în masă, expeditorii trebuie să păstreze date ce atestă aprobarea fiecarui destinatar de a primi astfel de mesaje înainte ca mesajele să fie trimise. Dacă astfel de dovezi nu există, COMBRIDGE poate considera, după propria sa apreciere, că aprobarea nu a fost obținută și va considera abuzivă utilizarea rețelei. COMBRIDGE nu este responsabil pentru conținutul nici unui mesaj, indiferent dacă mesajul a fost trimis de către un client COMBRIDGE.

2.1.6.3. Clienții COMBRIDGE sunt responsabili ca orice utilizator care beneficiază de serviciile COMBRIDGE să respecte aceste reguli de utilizare. Clienții COMBRIDGE vor fi răspunzatori pentru toate abuzurile directe sau indirecte, inclusiv pentru abuzurile clienților sau partenerilor Clienților COMBRIDGE realizate prin intermediul serviciilor puse la dispoziție de către COMBRIDGE.

2.1.6.4. Orice încercare de violare a securității rețelei sau de abuz sunt interzise. COMBRIDGE va investiga plângerile legate de aceste incidente și va coopera cu instituțiile legale pentru detectarea cauzelor și autorilor acestor incidente. Dacă COMBRIDGE primește o plângere, îndreptată către un Beneficiar al său (client al unui Beneficiar, partener al unui Beneficiar), aceasta va fi trimisă către client (Beneficiar) pentru a fi rezolvata. Dacă într-un interval de 24 (douăzeci și patru) de ore nu se primește nici un răspuns care să indice că problema a fost rezolvată, COMBRIDGE poate bloca traficul spre/de la adresa/adresele IP implicate în plângere până când COMBRIDGE este convinsă ca problema s-a rezolvat și că s-au luat măsuri de precauție pentru a preveni incidentele viitoare.

2.1.6.5. COMBRIDGE poate bloca traficul către IP-urile implicate în plângere, sau către toate IP-urile clientului, până este convins că s-au luat măsuri de siguranță de către Beneficiar pentru a nu se mai repeta incidentele.

2.1.6.6. Clienților care folosesc legătura la rețeaua COMBRIDGE pentru activități ce încalcă dispozițiile legale în vigoare sau viitoare și/sau prevederile prezentei Secțiuni sau clienților ori utilizatorilor care cu orice titlu folosesc rețeaua COMBRIDGE, li se poate supenda/bloca traficul care se realizează pe un anumit port TCP/IP sau li se poate suspenda serviciul furnizat pe o perioda nedeterminată, cu o notificare de 1(una) oră inainte sau imediat, fără notificare, în functie de gravitatea problemei și/sau în funcție de afectarea Rețelei ori a serviciilor COMBRIDGE. Dacă serviciul este oprit imediat, COMBRIDGE va încerca sa contacteze Beneficiarul cât mai curând posibil, pentru a-l informa despre situația apăruta.

2.1.6.7. Clienții care administrează un un domeniu Internet, au obligația de a configura două casuțe poștale: postmaster@domeniu.ro si abuse@domeniu.ro . Mesajele trimise către aceste adrese trebuie citite de persoane în măsură să ia decizii pentru soluționarea problemelor raportate. De asemenea, toți clienții sunt obligați să anunțe COMBRIDGE care sunt persoanele ce pot lua măsuri ca astfel de probleme să nu se mai întâmple.

2.1.6.8. In anumite cazuri, COMBRIDGE poate bloca traficul spre/dinspre anumite IP ce nu fac parte din reteaua COMBRIDGE, daca se considera ca acele IP-uri sunt folosite pentru a distribui SPAM, sunt “open relay” sau sunt folosite pentru obtine access la resurse ce nu au caracter public. In aceste cazuri nici un client nu va mai putea trimite/primi trafic de la acele adrese.

2.1.6.9. COMBRIDGE nu discuta decat cu clientii (Beneficiarii) sai directi. Este raspunderea Beneficiarului de a discuta cu clientii sai pentru a rezolva problemele aparute.

2.1.6.10. Beneficiarul are obligaţia:

a. să nu raspunda la cereri ARP venite din reţeaua COMBRIDGE pentru alte adrese IP decât cele alocate de către COMBRIDGE. În acest scop clientul este obligat: să nu seteze pe interfeţe direct conectate la reţeaua COMBRIDGE alte adrese IP decât cele alocate şi comunicate de către COMBRIDGE. În aceasta categorie intră şi adresele IP folosite de către Beneficiar în reţeaua locală şi care nu sunt separate printr-un echipament Layer 3 (router) de reţeaua COMBRIDGE să nu activeze pe nici o interfață direct conectată cu reţeaua COMBRIDGE opțiunea "proxy-arp" şi o va dezactiva pe echipamentele care o au activată în mod implicit (de exemplu: routerele marca Cisco).

b. să nu răspundă la cereride tipul BOOTP, DHCP şi alte cereri de configurare venite din reţeaua COMBRIDGE. În acest scop, dacă se folosesc astfel de servicii pentru reţeaua locală a Beneficiarului, ele trebuie dezactivate pe interfaţa direct conectată la rețeaua COMBRIDGE.

c. să nu trimită spre reţeaua COMBRIDGE cereri de modificare a rutelor pentru alte adrese de IP decât cele alocate de către COMBRIDGE sau aparţinând Beneficiarului. În acest scop, nu se vor activa şi folosi pe interfaţa direct conectate la rețeaua COMBRIDGE, protocoale de anunţare dinamică a rutelor, altele decât cele convenite cu COMBRIDGE, şi se vor dezactiva protocoalele de tip RIP/OSPF.

d. să nu trimită spre reţeaua COMBRIDGE pachete de tipul "ICMP redirect" pentru alte adrese IP decât cele alocate de către COMBRIDGE.

e. să evite trimiterea spre reţeaua COMBRIDGE a altor pachete de tip “broadcast” decât cele strict necesare (tipul ARP), acestea din urmă trebuind să respecte un algoritm de mărire a intervalului de interogare, care să ajunga la peste 1 (una) secundă în cazul în care nu se primeşte răspuns.

2.1.7. Recomandări

2.1.7.1. Beneficiarul trebuie să țină la curent COMBRIDGE, cu numele și adresele de contact pentru persoanele ce pot soluționa problemele descrise în prezenta Secțiune.

2.1.7.2. Beneficiarul trebuie să ia toate măsurile necesare astfel încât orice utilizator al serviciului furnizat acestuia de către COMBRIDGE să respecte prezentele reguli și obligațiile stabilite prin actele normative din domeniu.

2.1.7.3. Beneficiarul trebuie să investigheze rapid orice plângere care a fost primită de la COMBRIDGE.

2.1.7.4. Când Beneficiarul trimite mesaje de e-mail (poștă electronică) către o listă de destinatari, trebuie să se asigure că are confirmarea fiecărui destinatar care doreşte să primească mesaje sale.

2.1.8. Alte recomandări

● Instalarea unui software antivirus, păstrarea lui actualizat, verificând zilnic noile definiții de update-uri. Marea majoritate a software-urilor antivirus pot fi programate să facă acest lucru în mod automat.

● Asigurarea pentru ca toate patch-urile de securitate să fie instalate, deoarece în mod constant sunt descoperite noi vulnerabilități de Windows.

Virușii continuă să exploateze vechile vulnerabilități deoarece mulți utilizatori nu folosesc în mod regulat patch-uri. Nefolosirea patch-urilor nu va expune la risc doar propriul sistem.

Dacă un virus s-a infiltrat în sistemul calculatorului deoarece nu s-a instalat unul dintre patch-urile potrivite, toți cei din address book-ul personal devin următoarea țintă.

● Folosirea firewall, deoarece nici o conexiune la Internet nu este în siguranță fără acest firewall. Trebuie găsit un firewall pe care îl suportă conexiunea. Firewall-urile se vor dovedi utile chiar dacă, conexiunea la Internet este de tip dial-up. Dacă există conexiune la Internet de tip broadband (banda larga), sistemul va deveni mult mai vulnerabil atacurilor.

● Securizarea E-mail-ului. Trebuie să ne asigurăm că nu suntem expuși la infecții de către clientul E-mail. Atașamentele sunt doar o mică ecuație în această problemă. Dacă nu se reușește configurarea acestui serviciu, se recomandă aplicarea patch-urile și toate celelalte precauții cu privire la atașamente, deoarece cea mai slaba verigă o constituie Email-ul.

● Securizarea browser-ului. Dacă se foloseste Internet Explorer se poate profita de setările zonelor sigure pentru a asigura maximum de securitate la browser.

2.1.9. Limitarea responsabilității

COMBRIDGE nu poartă nici o responsabilitate pentru nerespectarea de către Beneficiar a obligațiilor legale, a celor contractuale, a prezentelor regului de utilizare și/sau a recomandărilor incluse în aceste reguli.

2.2. Acces Internet proprietate client

Incidentele si modificările pe serviciul de acces internet proprietate client intră in responsabilitatea clientului.

Responsabilii Combridge pot realiza o verificare preliminară doar dacă serviciul Smart CPE are un back-up 3G activat.

Pe acest serviciu nu se garanteaza niciun nivel de disponibilitate (SLA)

2.3. Back-up 3G

Inclus în serviciul **Smart CPE-A**, soluția de back-up vă oferă următoarele avantaje:

- Previne impactul operațional și pierderile de venituri ce ar putea avea loc în cazul în care o locație se deconectează;
- Costuri reduse;
- Trecere automată la conexiunea de back-up când circuitul principal prezintă disfuncționalități;
- Conectivitatea și datele nu sunt afectate fiindcă adresa IP nu se schimbă
- Trafic nelimitat;
- Viteză de transfer pentru primii 8GB este best effort (până la 225Mbps download si până la 50Mbps upload) și pentru ce depășește 8GB este maxim 128 kbps download / 64 kbps upload.

Combridge ofera serviciile indicate doar in aria de acoperire a Furnizorului de comunicații electronice comunicată de catre Managerul responsabil de Client, fie din initiativa Combridge, fie la cererea Clientului, oricând pe parcursul derularii contractului.

2.4. Sistemul Cloud management

NMS este un sistem de management enterprise-class disponibil in cloud ce permite crearea politicilor de lățime de bandă, monitorizarea centralizată fără a fi necesară introducerea in retea a unui echipament suplimentar.

3. Virtual Private Network (VPN)

Caracteristicile pachetului VPN:

- Configurarea tunelului VPN are la baza virtualizarea Vmware;
- Scalabilitate faţă de modificările de configuraţie şi efort minim necesar pentru reconfigurarea reţelei, în cazul suplimentării locaţiilor de acces din reţeaua clientului;
- Toate locaţiile de acces din reţeaua clientului sunt integrate în acelasi VPN folosind soluția VPN IPSec în cazul accesului internet proprietate client și cel furnizat de Combridge sau soluția MPLS VPN în cazul accesului internet furnizat de Combridge;
- Este ideal pentru conexiunile site-to-site;
- Securitate implicită a transmisiilor de date, prin rețeaua virtuală;
- Layer 3 IPsec VPN: se folosește procedeul NAT (network address translation) pentru maparea adreselor IP private permițând astfel stațiilor ce au IP-uri private sa se conecteze la Internet;
- Extinde politicile de securitate existente, în special cele referitoare la accesul la intranet, asupra angajaților mobili;
- Rutare: statică sau dinamică;
- Serviciile oferite pe rețeaua Combridge sunt servicii sigure şi de înaltă calitate;
- Monitorizare proactivă;
- Se achiziționează o singură dată și se poate folosi pentru un număr nelimitat de locații;
- Reducerea cheltuielilor alocate IT-ului şi buget previzibil;

VPN Gateway Virtual Appliance este proiectat pentru a simplifica terminarea rețelelor VPN pentru mii de locații de acces din rețeaua clientului într-un mod inovativ. Inima produsului este o aplicație software pentru echipamentele compatibile VMware; sufletul produsului este un concentrator VPN enterprise-class capabil sa termine mii de tunele destinate conectării la distanța a locațiilor de acces din rețeaua clientului.

Branch on Demand (Sucursală la cerere) este o soluție disponibilă în cloud ce simplifică implementarea, gestionarea (management-ul), securitatea și depanarea (troubleshooting-ul) pentru implementările la distanță. Punctul central îl reprezintă platformele Smart CPE. Datorită sistemului de operare robust, Smart CPE-ul nu necesită, practic, nicio altă intervenție din partea utilizatorului final decât pornirea și conectarea la Internet. Odată pornit și conectat la Internet echipamentul își va găsi automat NMS-ul, ce poate fi localizat în cloud sau în rețeaua locală, își va descărca politicile de securitate stabilind astfel conexiunea la VPN. În

numai câteva minute noua locație va fi activă si vizibilă în VPN nefiind necesară descarcarea configurației pentru fiecare dispozitiv sau instruirea utilizatorilor finali pentru folosirea rețelei VPN.

Datorită politicilor unificate atât pentru comunicarea pe fir cât și pentru cea wireless configurarea oricărei rețele pentru o gamă largă de clienți devine ușor de realizat. Când echipamentul devine online, NMS-ul îi transmite în mod automat, pe baza parametrilor dispozitivului, configurația. NMS-ul este localizat în afara rețelei locale, iar disfuncționalitățile rețelei WAN nu influențează rețeaua locală sau WLAN. Având în vedere ca NMS-ul are o singură interfața centralizată pentru configurarea si gestionarea AP-urilor si router-elor, gestionarea a mii de dispozitive este literalmente la fel ca gestionarea unui singur dispozitiv.

4. Soluția Corporate Communication

Este disponibilă in 2 variante:

- ✓ **Corporate Communication Solution entry (CCS-E) până la 20 de utilizatori.**
- ✓ **Corporate Communication Solution advanced (CCS-A) pentru un număr nelimitat de utilizatori**

- Voce, Video, Fax, Chat profesional integrat cu ușurința cu server-ul de mail, server-ul web, server-ul de securitate si aplicațiile business.
- CCS-E include 1 (un) VPS-A
- CCS-A include 1 (un) VPS-S
- **Principalele caracteristici ale CCS (funționalitățile pot fi opționale):**

4.1. IP PBX

- Poate înlocui în totalitate centrala tradițională (PBX).
- Oferă o gamă largă de servicii, inclusiv un trunk de voce cu 100 linii, 100 numere de telefon, suport pentru telefon SIP, suport pentru Soft Phone, Fax2Mail&Mail2Fax, gestionarea cozii de apel (queue management), redirecționare apel (follow me), programarea unui apel (call scheduling), preluare apel (call pick-up), blocarea unui apel (call blocking), IVR, ENUM, statistici apel (call statistics), transfer de apel (call parking and transfer), muzică apel in așteptare (on-hold music), teleconferință (call conference). Traficul de voce generat nu este inclus in taxa lunară, tarifarea se realizează conform listei de prețuri SIP TRUNK în vigoare publicată pe site-ul www.combridge.ro.
- Permite configurarea ușoară a grupurilor de apel și a claselor de acces.
- Funcția DISA permite accesul din afara biroului la toate funcționalitățile telefonului ca și când ai fi in birou.
- Cu ajutorul serviciului Fax2Mail orice fax primit este redirecționat către o adresă de mail predefinită. Un mail este trimis către un număr de fax prin serviciul Mail2Fax. Un fișier PDF se poate anexa unui mail și se poate trimite către un număr de fax prin simpla folosire a clientului de mail sau prin web-mail.

Follow me – redirecționarea unul apel configurată de la extensia destinație (ex. Dacă ai extensia 200 si lucrezi de la un alt birou, poți ridica receptorul extensiei unde ești prezent, să tastezi codul pentru follow me, extensia ta, in acest caz 200, și parola extensiei, iar apelurile către extensia 200 vor fi redirecționate către noua extensie.
Call schedule (Programare apel) – denumit și distribuție de apeluri conform programării.
Call Parking (Apel in așteptare) – permite oricărui utilizator sa pună apeluri in așteptare.
Call Transfer (Transfer apel) – permite oricărui utilizator sa transfere apelul către o altă destinație.
Call forwarding (Redirecționare apel) - este o funcționalitate ce permite utilizatorilor sa își redirecționeze apelurile primite catre o altă destinație ce poate fi atât număr fix cât și mobil.
Call Pickup (Preluare apel) - preluarea unui apel care sună la un alt telefon din grupul de preluare.
Conference calls (Teleconferințe) - adăugarea intr-un apel a unuia sau mai multor participanți

Call blocking (Blocare apel) – permite unui utilizator sa blocheze apelurile primite de la un anumit număr de telefon.
Hold-on music (Muzică apel in așteptare) – redarea unei melodii inregistrate care să umple liniștea unui apel ce a fost pus in așteptare.
Direct inward system access – **DISA** este o funcționalitate prin care un apelant, după ce a tastat codul printr-un meniu, primește un ton de apel pentru a accesa o parte sau toate funcționalitățile PBX, cum ar fi realizarea unui apel in străinătate sau adresarea unui mesaj vocal.
Interactive Voice Response or **IVR** – permite clienților sa interacționeze, in timp real, cu un robot prin apăsarea tastelor corespunzatoare meniului vocal oferit folosind tonuri multifrecvență (DTMF).
ENUM – reprezinta convertirea unui număr de telefon intr-o adresă IP.
Call statistics (statistici de apeluri) – reprezintă o detaliere a apelurilor companiei dându-i clientului posibilitatea să aibă o imagine de ansamblu.
Queue Management – ajută la organizarea apelurile din coadă.

4.2. Conferința dinamică și statică

Conferințele statice și dinamice sunt funcționalități opționale configurate de Suportul tehnic Combridge la solicitarea clientului.
În cazul unei conferințe statice se alocă numere de telefon si PIN-uri preconfigurate (ex: nr tel: 0310800xxx, PIN: 6589#), iar în cazul celei dinamice se preconfigureaza doar numărul de telefon, PIN-urile rămân la alegerea clientului.

Mod de folosire :

4.2.1. Conferința statică – se folosesc numărul de telefon și PIN-ul furnizate de Combridge (ex. 0310800xxx. PIN 6589#)

a. Fiecare participant sună la numărul de telefon presetat (ex. 0310800xxx) folosind +40 (ex. +40310800xxx) dacă sună din afara țării.
b. Participantul va fi rugat să introducă numărul PIN al conferinței și va tasta PIN-ul preconfigurat urmat de tasta # (ex. 6589#)
c. Participantul va fi rugat sa își spună numele după bip și după ce a rostit numele să apese din nou tasta diez (#)
d. Participantul este întrebat de alte trei opțiuni :

i. Să apese 1 pentru acceptare nume și intrare în conferință
ii. Să apese 2 pentru ascultare nume
iii. Să apese 3 pentru înregistrare nume din nou (în cazul în care nu s-a auzit bine prima data)

Pașii i, ii si iii pot fi repetați până când participantul apasă tasta 1 și acceptă numele înregistrat fiind introdus în conferință.

4.2.2. Conferința dinamică – se folosește numărul de telefon furnizat de Combridge (0310800xxy)
a. Fiecare participant sună la numarul furnizat de suportul tehnic Combridge (ex. 0310800xxy sau +40310800xxy dacă sună din afara țării)
b. Participantul este rugat să introducă ID-ul conferinței urmat de tasta diez #

Primul participant sau cel ce organizează conferința poate seta ID-ul conferinței, important este ca numărul de telefon și ID-ul conferinței să fie transmis tuturor participanților. Dacă unul din participanți greșește ID-ul, inițiază, defapt, o nouă conferință.

c. Participantul va fi rugat să introducă numarul PIN al conferinței și va tasta PIN-ul urmat de tasta #.

Primul participant sau cel ce organizează conferința va seta PIN-ul conferinței urmat de tasta # (nu trebuie să fie un PIN fix, pot fi 3 sau 4 cifre, la alegere, urmate de tasta #). Ceilalți participanți vor introduce PIN-ul creat de primul participant la conferință, PIN ce a fost transmis in prealabil către toți participanții.

d. Participantul va fi rugat să își rostească numele după bip și după ce a spus numele să apese din nou tasta diez (#)
e. Participantul este întrebat de alte trei opțiuni :

i. Să apese 1 pentru acceptare nume și intrare în conferință
ii. Să apese 2 pentru ascultare nume
iii. Să apese 3 pentru înregistrare nume din nou (în cazul în care nu s-a auzit bine prima data)

Pașii i, ii si iii pot fi repetați până când participantul apasă tasta 1 și acceptă numele înregistrat fiind introdus în conferință.

La numărul setat pentru conferința dinamică pot avea loc, simultan, oricâte conferințe se doresc, important este ca fiecare conferință să aibă setat un PIN propriu astfel încât participanții unei conferințe să nu participe la o conferință în derulare, de preferat ar fi să se folosească PIN-uri mai complexe pentru conferințele de importanță majoră.

4.3. Hosting

Virtual hosting (Găzduirea virtuală) este o soluție simplă, flexibilă, de inaltă calitate ce oferă posibilitatea de a găzdui, in limita spațiului de pe discul unde CCS este configurat, server de mail, server de FTP și un număr nelimitat de domenii și site-uri web fără a aloca resurse dedicate responsabile de mentenanța soluției de găzduire.

Soluția de email și groupware permite clienților să schimbe mail-uri, să își gestioneze calendarul și agenda de adrese. Acest serviciu include antivirus, filtrare anti-spam, actualizări, acces la browser, client de email si integrarea calendarului. Îți poți accesa mail-urile, contactele si, de asemenea, consulta, gestiona si distribui calendarul si activitățile pe o platformă sigură și complet integrată.

4.4. Security

Platforma de securitate este o metodă scalabilă de a gestiona riscurile de securitate cu care se pot confrunta aplicațiile companiei folosind un firewall de filtrare a pachetelor IP, proxy explicit, filtrarea conținutului si reverse proxy.

Proxy mode poate fi folosit pentru orice serviciu important precum STMP, HTTP/HTTPS, FTP, Skype și Messenger.

Filtrarea conținutului (**Content filtering**) poate fi aplicată pentru filtrarea site-urilor pe baza domeniului precum reclame, jocuri, continut dedicat adulților, etc.

4.5. Server de domeniu (Domain Server)

Permite administratorilor sa își segmenteze dinamic, fără costuri suplimentare, sistemul Windows in rețele izolate si sigure bazate pe politici de securitate folosind protocolul **LDAP** și totodată sa realizeze o integrare

cu **Active Directory**, **Radius Server**, protocolul **DHCP**, protocolul **DNS**, **server-ele de imprimantă si baze de date.**

4.6. Protecție DDoS (DDoS Protection)

Un atac cibernetic de tip DoS (denial of service= refuzul, blocarea serviciului) sau DDoS (Distributed Denial of Service = blocarea distribuită a serviciului) este o încercare frauduloasă de a indisponibiliza sau bloca un server/serviciu. Deși mijloacele și obiectivele de a efectua acest atac sunt foarte diverse, în general acest atac este efectul eforturilor intense ale unei sau a mai multor persoane de a împiedica un server/serviciu de a funcționa eficient, temporar sau nelimitat.

Folosind senzori pentru a detecta atacurile la limita rețelei, fiecare IP ce primeste trafic din Internet prin rețeaua Combridge poate fi protejat de orice tip de atac DDoS.

În momentul in care se detectează un trafic suspect, traficul către acel IP este redirecționat către un Cloud securizat, atenuând impactul către client și păstrând o latență constantă. Procesul de detecție, filtrare si deturnare a rutei default este unul complet automat a cărui eficacitate este subliniată de contramăsurile luate in timp real total transparente clientului final.

Resursele ce urmează a fi protejate sunt decise pe baza unui route-map special și a unui anunț de bgp. Route-map-ul trebuie actualizat cu ASN-urile/AS-set-urile de care aparțin prefixele ce urmează a fi protejate. De asemenea, prefixele protejate trebuie să fie anunțate prin BGP către Combridge.

Doar traficul real este livrat către echipamentul clientului.

5. VPS – Virtual Private Server (Server virtual privat)

- Serverele VPS sunt configurate pe un server fizic instalat in București intr-un centru de colocare Tier 3 securizat, cu back-up-uri ce se realizează in mod automat si capabilități de recuperare in caz de dezastru.
- Sisteme de operare disponibile: Centos, UBUNTU, Free BSD, Debian, Windows
- Performanță optima, securitate si disponibilitate maximă
- Este disponibil in VPN-ul clientului
- Putere de procesare suplimentară din cloud
- 3 produse:
  - VPS Easy (**VPS-E**)
  - VPS Advanced (**VPS-A**)
  - VPS Star (**VPS-S**)
- Fiecare VPS include 1 (o) adresă publica IPv4 or Ipv6
- 99.9% SLA
- Caracteristici:

	Easy	Advanced	Star
Stocare	Da	Da	Da
Tip de stocare	HDD	SSD	SSD
Spațiu de stocare	10GB	30GB	100GB
RAM garantat	1GB	4GB	16GB
RAM maxim	2GB	8GB	20GB
CPU	1c @ 2 GHz	1c @ 2 GHz	1c @ 2 GHz
vCPUs	1	1	2
Trafic	Nelimitat	Nelimitat	Nelimitat
Network port	1Gbit	1Gbit	1Gbit

Pentru instanțele Windows trebuie alocat un spațiu minim de stocare de 50GB.

- Resursele pe cele 3 VPS-uri se pot suplimenta, la cerere, cu multiplu de 2GB RAM și multiplu de 100GB spațiu de stocare.

5.1. Politica de utilizare a serviciilor VPS

5.1.1. Beneficiarul nu are permisiunea să utilizeze rețeaua şi serviciile Furnizorului pentru a transmite, a distribui sau a stoca material (a) care încalcă vreo lege sau vreun regulament aplicabil, inclusiv legislaţia altor ţări de unde accesul către VPS este posibil (b) într-o manieră care să ducă la încălcarea copy-right-ului, a mărcii, a secretului comercial sau a altor drepturi de proprietate intelectuală sau a dreptului de intimitate, la publicitate sau a altor drepturi personale ale altor părți, (c) dacă acesta este necinstit, obscen, defăimător, calomniator, amenințător, abuziv sau conține un virus, worm, cal Troian, sau orice altă componentă de natură să producă defecţiuni, (d) conține oferte frauduloase de bunuri sau servicii sau alte materiale promoționale care conțin afirmații, pretenții sau reprezentări false, de natură să înșele sau să inducă în eroare sau (e) în general, într-o manieră care poate angaja răspunderea penală sau civilă a Furnizorul sau a oricărui angajat al acesteia.

5.1.2. Furnizorul nu-şi asumă nicio responsabilitate pentru vreun material creat sau accesibil pe sau prin rețelele şi serviciile Furnizorului care nu este expediat de sau la cererea Furnizorului. Furnizorul nu monitorizează sau exercită niciun control editorial asupra vreunui asemenea material, dar îşi rezervă dreptul de a face acest lucru în măsura în care îi este permis de legea aplicabilă.

5.1.3. Furnizorul nu este responsabil pentru conținutul niciunui web site, altul decât cele care aparțin Furnizorului.

5.1.4. Utilizatorii - Clienţi nu pot expedia mesaje care nu au fost solicitate pe e-mail, inclusiv, fără a se limita la, pachete de reclame.

5.1.5. (1) Beneficiarul se obligă să nu încalce sau să încerce să încalce securitatea Rețelei Furnizorului a Serviciilor, inclusiv, dar fără a se limita la: (a) accesarea de date care nu sunt destinate Clientului sau pătrunderea într-un server sau cont pe care Beneficiarul nu are permisiunea să-l acceseze, (b) încercarea de a scana sau proba vulnerabilitatea unui sistem sau a unei rețele sau de a încălca securitatea acestuia/acesteia sau măsurile de autentificare fără a fi autorizat în mod corespunzător, (c) încercarea de a interfera cu, de a întrerupe sau a face inutilizabil Serviciul unui alt utilizator, gazdă sau rețea, inclusiv, fără a se limita la mijloace de supraîncărcare, „flooding", „mailbombing" sau „spaming", adică trimiterea de cantități mari de e-mailuri sau altfel de informaţii către o adresă de e-mail individuală sau către un alt utilizator al Serviciului, (d) contrafacerea oricărui "header" TCP/IP sau a oricărei părți din informaţia cuprinsă în aceasta odată cu expedierea prin e-mail sau către un grup Usenet sau declanșarea oricărei acțiuni în vederea obținerii de servicii la care Beneficiarulnu are dreptul.
(2) Pentru protejarea Rețelei Furnizorului, a resurselor Furnizorului, precum şi a celorlalți Clienți ai Furnizorului, în cazul unor atacuri de tip „Denial-of-Service" având ca țintă adrese de Internet, Furnizorul îşi rezervă dreptul de a lua măsurile ce se impun pentru minimizarea efectelor unor astfel de incidente. Măsurile pot include, fără a se limita la, blocarea temporară în întreaga Rețea a Furnizorului a adreselor sau claselor de adrese supuse atacului.
(3) Furnizorul își rezervă dreptul să șteargă orice informaţie pe care Beneficiarula introdus-o în sistemul său şi care poate cauza căderea sau funcţionarea necorespunzătoare a Rețelei Furnizorului. (4) Beneficiarulrăspunde pentru protecția sistemului său informatic și pentru integritatea datelor introduse în sistemul Furnizorului.

5.1.6. Nu este permisa utilizarea următoarelor scripturi pe serverele Furnizorul:
• UltimateBBS • Orice script sau platformă care permite Content Sharing (torrent, dc, ș.a.m.d.) • IkonBoard • Toate versiunile de forum YABB • Scripturi pentru proxy • Scripturi pentru IRC (ircbots, psybnc, ș.a.m.d.) • Anonimizator • Phishing • Chat room-uri, fără a include scripturile standard din panoul de control • PhpShell şi scripturi similare pentru executarea de comenzi - FormMail • Alte scripturi şi aplicaţii care au vulnerabilităţi sau comportament periculos. • Instalarea instanţelor de jocuri (Counter Strike, Half-Life, Minecraft, ș.a.m.d.) • Instalarea şi utilizarea Shoutcast sau orice software similar de audiostreaming • Instalarea şi utilizarea Wowza sau orice software similar de videostreaming • Instalarea şi rularea de mirror-uri publice • Site-uri de hacking, warez sau care promovează activităţi ilegale sau interzise prin lege • Instalarea şi rularea web-spiders sau crawlers • Instalarea/Rularea

scripturilor care generează atacuri DDOS • Scripturi care testează şi/sau exploatează vulnerabilităţi ale oricăror sisteme de operare, echipamente, platforme sau site-uri web.
5.1.7. Furnizorul va pune în aplicare orice cereri şi decizii ale organelor şi instituţiilor abilitate, inclusiv organe penale şi instanţe judecătoreşti, privind refuzul accesului Clientului la Serviciu, , furnizarea oricăror informaţii despre Client (inclusiv date identificare, metoda de plată, facturi). În aceste situaţii nu există obligaţia informării prealabile a Clientului şi nici îndeplinirea vreunei alte formalităti, iar Furnizorul nu poate fi ţinută responsabilă pentru încălcarea confidenţialităţii.
5.1.8. Beneficiarul declară că a înţeles şi acceptă că este singurul responsabil, nelimitat, pentru încălcarea oricărei interdicţii menţionate mai sus, şi că în aceste cazuri Furnizorul are dreptul să schimbe, blocheze, suspende, înceteze furnizarea Serviciului şi să şteargă conţinutul Serverului, fără îndeplinirea vreunei formalităţi prealabile, Beneficiarulurmând a despăgubi de îndată Furnizorul pentru orice şi toate prejudiciile cauzate prin încălcarea acestor prevederi.
5.1.9. Beneficiarul declară, acceptă şi se obligă să respecte orice notificări, avertizări transmise de către Furnizor sau publicate pe Site in timpul utilizării Serviciilor.
5.1.10. Beneficiarul declară că a înţeles şi acceptă că Serviciul furnizat este exclusiv în proprietatea Furnizorului şi că drepturile de proprietate intelectuală şi industrială pentru orice software, design, program sau orice alt conţinut în legătură cu Serviciul aparţine exclusiv Furnizorului. În cazul constatării oricărei încălcări a acestor drepturi ale Furnizorului, de către Client, Furnizorul îşi rezervă dreptul să înceteze de îndată furnizarea Serviciului, să şteargă conţinutul Serverului şi totodată să demareze orice proceduri legale pe care le consideră necesare.

6. Managed LAN

Soluție completă ce cuprinde furnizarea infrastructurii IT, administrarea și monitorizarea acesteia precum și dezvoltarea de soluții personalizate de recuperare in caz de dezastru prin care clientul deține controlul deplin al aplicațiilor și a datelor.

Caracteristici:

- O nouă infrastructură
- Management in Cloud
- Politici unificate atât pentru comunicarea pe fir cât și pentru comunicarea wireless
- Securitate enterprise-class
- PoE
- Implementare zero-touch
- Qos
- 24/7/365 suport tehnic
- Monitorizare proactivă
- Schimbarea echipamentului in Next Business Day (următoarea zi de lucru)

Echipamente:

Small Branch 8 port switch (MLAN-8P)
Ideale pentru Retail/Small Branch, Camere de conferință (Fanless, 1GE Uplinks, PoE)
Porturi PoE: 8PoE/PoE+GE
Putere maximă PoE: 124 W
Capacitate Uplink: 2 x 1GE Combo (SFP sau Cupru)
Capacitate de comutare: 20Gbps

Enterprise Class 48 port switch (MLAN-48P)
Enterprise Class Premium
Ideale pentru: implementarea campusurilor mici si mijlocii (Buget mare de putere, Uplink-uri 10GE, pentru clienți pregătiți pentru HMNG) Ex: K-12, Întreprinderi, Universități
Porturi PoE: 48 PoE/PoE+GE
Putere maximă PoE: 740W
Capacitate Uplink: 4 x 10GE SFP+

Enterprise Class 24 port switch (MLAN-24P)
Enterprise Class Premium
Ideale pentrur: : implementarea campusurilor mici si mijlocii (Buget mare de putere, Uplink-uri 10GE, pentru clienți pregătiți pentru HMNG) Ex: K-12, Întreprinderi, Universități
Porturi PoE: 48 PoE/PoE+GE
Putere maximă PoE: 370W
Capacitate Uplink: 4 x 10GE SFP+
Capacitate de comutare: 128Gbps

Coduri de comandă: ***MLAN-8P-SEL-1YR/3YR, MLAN-24P-E-SEL-1YR/3YR, MLAN-24P-A-SEL-1YR/3YR, MLAN-48P-SEL-1YR/3YR, MLAN-8P-CON-1YR/3YR, MLAN-24P-E-CON-1YR/3YR, MLAN-24P-A-CON-1YR/3YR, MLAN-48P-CON-1YR/3YR***

7. Managed WLAN

Permite utilizarea unei rețele wireless pentru a crea un mediu de lucru mai flexibil, în scopul de a spori flexibilitatea afacerii.

Caracteristici:

- Management in cloud
- Politici unificate atât pentru comunicarea pe fir cât și pentru comunicarea wireless
- Securitate enterprise-class
- PoE
- Implementare zero-touch
- Interoperabilitate cu diverse brand-uri de pe piață
- 24/7/365 suport tehnic
- Monitorizare proactivă
- Schimbarea echipamentului in Next Business Day (următoarea zi de lucru)

O excelentă flexibilitate dată de 10 tipuri diferite de AP-uri:

1. **MWL-122** - Basic Dual Band Access Point - 2x300 Mbps Internal Antenna (Indoor; Dual Radio 802.11n or 11n/ac; TPM Security Chip & PPSK; 1xGEth interface; 1xPOE; USB; 0°C - 40°C)
2. **MWL-130** - High Density Dual Band Access Point - 300+867 Mbps Internal Antenna (Indoor; Dual Radio 802.11ac/n Wave 1; TPM Security Chip & PPSK; 1xGEth interface; 1xPOE; no USB; 0°C - 40°C)

3. **MWL-230** - High Density Dual Band Access Point - 450+1.3 Gbps Internal Antenna (Indoor; Dual Radio 802.11ac/n Wave 1; TPM Security Chip & PPSK; 2xGEth interface with Link Aggregation; 1xPOE; USB; 0°C - 40°C)
4. **MWL-245** - High Density Dual Band Access Point - 450+1.3 Gbps Ext. Antenna (Indoor; Dual Radio 802.11ac/n Wave 2; TPM Security Chip & PPSK; 2xGEth interface; 1xPOE; USB+BLE; 0°C - 50°C)
5. **MWL-250** - High Density Dual Band Access Point - 1.3+1.3 Gbps Int. Antenna (Indoor; Dual Radio w/ a Software Selectable Radio 802.11ac Wave 2; TPM Security Chip & PPSK; 2xGEth interface with Link Aggregation; 1xPOE; USB+BLE; 0°C - 40°C)
6. **MWL-550** - Extreme Performance Dual Band Access Point - 1.7 +1.7 Gbps Int. Antenna (Indoor; Dual Radio 802.11ac/n Wave 1; TPM Security Chip & PPSK; ; 2xGEth interface with Link Aggregation; 2xPOE; USB+BLE; 0°C - 40°C)
7. **MWL-1130** - Outdoor Access Point IP67 - 300 + 867 Mbps Ext Antenna (Outdoor; Dual Radio 802.11ac/n Wave 1; TPM Security Chip & PPSK; 1xGEth interface; 1xPOE; no USB; - 40°C - 55°C)

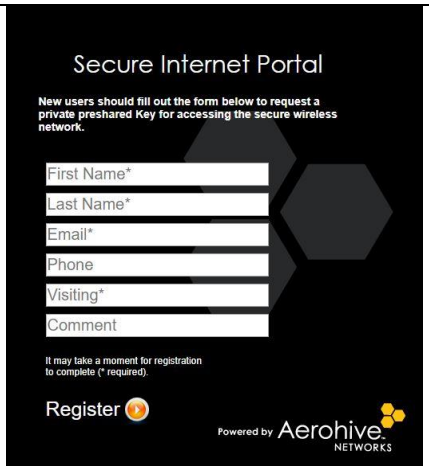
Coduri de comandă: ***MWL-122-CON-1YR, MWL-130-CON-1YR/3YR, MWL-230-CON-1YR/3YR, MWL-245-CON-1YR/3YR, MWL-250-CON-1YR/3YR, MWL-550-CON-1YR/3YR, MWL-1130-CON-1YR/3YR, MWL-122-SEL-1YR, MWL-130-SEL-1YR/3YR, MWL-230-SEL-1YR/3YR, MWL-245-SEL-1YR/3YR, MWL-250-SEL-1YR/3YR, MWL-550-SEL-1YR/3YR, MWL-1130-SEL-1YR/3YR***

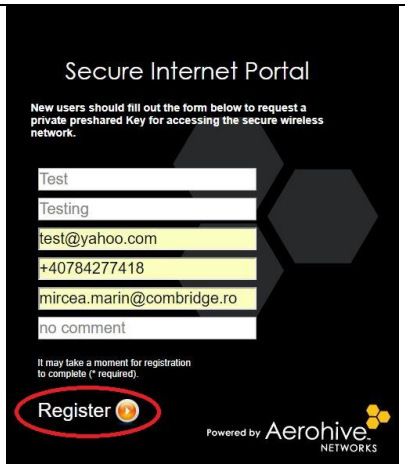
7.1. Manual de Auto-Înregistrare

Se realizează conectarea la Rețeaua Wireless de inregistrare și se va deschide automat o pagină de internet unde se vor introduce detaliile de conectare primite de la Combridge. În cazul în care există mai multe locații fiecare locație va avea o denumire proprie a rețelei de înregistrare, ex: nume client-Guest-Ploiesti-Registration, nume client-Guest-Constanta-Registration, etc. Toate rețelele vor adăuga utilizatorii in aceeași bază de dateș utilizatorii creați au valabilitate 7 zile și se vor putea conecta în orice locație.

Se vor completa campurile din pagina de web, ca in exemplu de mai jos dupa care vom da click pe register:

First Name: Test;
Last Name: Testing;
Email: test@yahoo.com (nu va trimite mail cu detaliile de conectare);
Phone: 1234567 (nu va trimite sms);
Visiting: mircea.marin@Combridge.ro (nu va trimite mail de confirmare);
Comment: (nu este obligatoriu).





Se va afișa pe ecran parola de conectare și rețeaua la care ne vom conecta pentru acces la internet.

NOTĂ: Parola trebuie copiată și salvată într-un fișier deoarece nu există posibilitatea de a o salva automat.

Se va realiza conectarea la rețeaua de internet guest utilizându-se parola furnizată de portalul Secure Internet la înregistrare, conform pașilor menționați în cadrul acestui capitol, și se dă click pe Next.

8. Telefoane (Voice Headsets)

8.1. Basic (VHB)

VHB1610 - GXP1610: 1 linie; conferință în 3 direcții; securitate: SIP/TLS, SRTP, AES-256, 802.1x.
VHB303 - SPA303-G2: 3 linii; conferință în 3 direcții; securitate: SIP/TLS.
VHB19P - T19P: 1 linie; conferință în 3 direcții; securitate: SRTP, TLS.

8.2. Medium (VHM)

VHM1628 - GXP1628: 2 linii; conferință în 3 direcții; Gigabit Port; Securitate: SIP/TLS, SRTP, AES-256, 802.1x.
VHM514 - SPA514G: 4 linii; conferință în 3 direcții; Gigabit Port; Securitate: RFC 1321; AES-256; SIP/TLS; SRTP
VHM23G - T23G: 3 linii; conferință în 3 direcții; Gigabit Port; Securitate: SRTP, TLS

8.3. High End (VHHE)

VHHE2170 - GXP2170: 12 linii; conferință în 5 direcții; Gigabit Port; Bluetooth; Securitate: SIP/TLS; SRTP

VHHE8861 - 8861: până la 10 linii; conferință în 3 direcții; Gigabit Port; Bluetooth; Securitate: AES; SIP/TLS; SRTP
VHHE29G - T29G: 12 linii; conferință în 3 direcții; Gigabit Port; Bluetooth; Securitate: AES-256; SIP/TLS; SRTP

8.4. Extension Set (VHEX)

VHEX2000 - GXP2200EXT: compatibil cu GXP2170
VHEX8800 - CP-BEKEM: compatibil cu Cisco 8861
VHEX20 - EXP20: compatibil cu Yealink T29G

Coduri de comandă: ***VHB1610, VHB303, VHB19P, VHM1628, VHM514, VHM23G, VHHE2170, VHHE8861, VHHE29G, VHEX2000, VHEX8800, VHEX20.***

9. Linkyfi

Linkyfi este o platformă destinată hotspot-urilor publice care combină gestionarea accesului, în calitate de vizitator, la WiFi și marketing-ul WiFi. Este un serviciu eficient care imbunătățește experiența WiFi a utilizatorilor finali.

Linkyfi este un instrument simplu de marketing care utilizează mecanismul accesului condiționat la Internet pentru a colecta date despre utilizatorii săi. Pentru a naviga gratuit pe Internet, clientul, încurajat de posibilitatea de a beneficia de o reducere sau de alte oferte atractive, se conectează la platforma Linkyfi. La conectare, clientului i se oferă posibilitatea de a alege modul de accesare a WiFi-ului gratuit - prin introducerea numărului de telefon sau a adresei de e-mail, conectarea prin conturile media sociale sau prin completarea unui scurt chestionar. O analiză aprofundată a informațiilor despre clienți permite proprietarului companiei să creeze și să trimită campanii publicitare personalizate clienților la adresa de email sau numărul de telefon furnizat. În plus, clientului i se poate oferi posibilitatea de a folosi meniul virtual, puncte virtuale/ștampile virtuale sau navigarea în locuri selectate. Platforma Linkify oferă o gamă largă de posibilități, fiind potrivită pentru diverse facilități, cum ar fi hoteluri, restaurante, aeroporturi, gări, mall-uri, cinematografe sau chiar evenimente în masă.

Funcționalități și beneficii:

- Studii de piață, rapoarte, statistici care oferă informații fiabile despre fiecare client, astfel încât proprietarul afacerii să poată ajusta în mod adecvat ofertele în funcție de nevoile clientului.
- Campanii de promovare adresate fiecărui client în parte, astfel încât să se poată realiza un contact direct cu clientul.
- Ștampilele virtuale reprezintă cardurile de loialitate ale generației viitoare, scopul acestora fiind de a crește atractivitatea brand-ului și de a avea o relație îmbunătățită cu clientul.
- Campanii personalizate de publicitate care sunt ușor de pregătit și de adaptat nevoilor fiecărui client și care asigură o eficiență sporită a campaniilor publicitare.
- Publicitatea pe mobil oferă proprietarului companiei posibilitatea de a transmite campanii publicitare direct pe mobilul clientului, asigurând o creștere a gradului de conștientizare a brand-ului în rândul clienților
- Localizarea interioară colectează informații despre modul și direcția de mișcare a fiecărui client, optimizând spațiul de vânzări și publicitate, sporind eficiența personalului.
- Licența se achiziționeaza o dată pe an și este disponibilă atât in varianta de 1 an cât și in cea de 3 ani.
- Produsul este disponibil in 3 variante:

- **Linkyfi Basic** (LBA/C/1 și LBA/C/3)
- **Linkyfi Plus** (LPL/C/1 și LPL/C/3)
- **Linkyfi Pro** (LPR/C/1 și LPL/C/3)

Caracteristici

Aplicații	Funcții	Basic	Plus	Pro
Tablou de comandă	Ultimele 24h – Clienți noi/Clienți ce au revenit	+	+	+
	Timpul mediu			
	Vizite			
	Istoricul și histograma conexiunilor			
	Clienți logați			
	Tipul de logare			
Portalul Captive	Editor CP	+	+	+
Marketing	Chestionare	-	+	+
	Interfață wizard			
	Raport			
	Campanii de marketing			
	Campanii de zile de naștere			
	Publicitate			
	Loializare			
	Rezultate			
Marketing geografic	Localizare interioară	-	-	+
	Editor			
	Hărți de acoperire (Heatmaps)			
	Modul de mișcare			
	KPI-uri pentru grupuri definite			
	Marketing bazat pe evenimente			
	Portaluri Captive			
	SMS			
	email			
	Postări pe Facebook			
Statistici	Clienți logați	-	+	+
	Trafic global			
	Demografie			
	Istoricul și histograma conexiunilor			
	Sisteme de operare			
	Dispozitive			
	Informații personale			
Multi-tenancy (interfață destinată mai multor clienți)	Date agregate pe nivel în cadrul organizației	-	+	+
	Permisiuni per unitate			
	Permisiuni per user			
Portofel Linkyfi		-	+	+

- Nu este conținut de produs + Este conținut de produs

10. Network management (administrarea rețelei)

- Access network management - MWL-CMBW-ANM – licență HiveManager NG Perpetual pentru un (1) dispozitiv de tip AP sau switch. Licența se achiziționează anual.
- Routing network management - MWL-CMBW-RNM - licență HiveManager Classic Perpetual pentru un (1) dispozitiv de tip AP, router sau switch. Licența se achiziționează anual.

10.1. MWL-CMBW-ANM

Aplicația virtuală Access network management este o versiune on-premises, care este de obicei implementată în rețeaua privată a clientului, în centrul de date al clientului. Dispune de aceeași funcționalitate de gestionare a rețelei la nivel de întreprindere ca și versiunea cloud publică, NMS, menționată în capitolele anterioare. Diferența constă în caracteristicile de instalare și administrare specifice implementărilor din locația clientului. Printre avantajele cheie se numără:

- Tabloul de comandă: panou vizual intuitiv, cu filtre contextuale pentru o imagine de ansamblu cuprinzătoare a dispozitivelor rețelei, carduri de stare cu KPI în rețea, utilizare a aplicațiilor și a datelor, precum și activitatea utilizatorilor.
- Vizibilitatea și controlul aplicațiilor: Vizibilitatea și controlul utilizării aplicațiilor în rețea, pentru aplicații profesionale și recreative.
- Implementare simplificată: Fluxuri de lucru pentru crearea și implementarea politicilor de rețea, cu configurație opțională avansată.
- Monitorizare: vizualizarea în timp real a dispozitivelor, clienților, alarmelor și evenimentelor. Abilitatea de a colecta informații despre dispozitive direct din interfața de monitorizare.
- Depanarea: interfață optimizată Help-Desk pentru a interoga istoricul unui client cât si problemele acestuia în timp real cu date concrete pentru a reduce escaladarea și a oferi o experiență mai bună utilizatorilor finali.
- Administrarea unificată a rețelei: Gestionarea cu o singură consolă de administrare atât a dispozitivelor fără fir (wireless) cât și a celor cu fir.
- Open APIs: acces la API-uri pentru servicii de monitorizare, identitate și configurare.
- Acces invitat: Îmbarcarea și gestionarea dispozitivelor personale pentru vizitatori și angajați.

10.2. MWL-CMBW-RNM

Sistemul de administrare Routing network management permite crearea de politici simple, actualizări de firmware, actualizări de configurație și monitorizare centralizată de la o singură consolă. Acest sistem combină AP-urile, router-ele si switch-urile cu o suită de protocoale de control cooperativ și funcții pentru a oferi un acces unificat, atât wireless cât și pe fir, care asigură o politică consistentă, permisiuni și securitate bazată pe identitatea și tipul dispozitivului, indiferent de locația utilizatorului. Routing network management oferă o consolă de gestiune centralizată pentru întreaga rețea, care permite o politică globală, configurarea și monitorizarea cu vizibilitate completă a mii de AP-uri, routere și switch-uri. Routing network management reduce costurile de operare prin accelerarea implementării, configurarea și monitorizarea întregii rețele.

Printre avantajele cheie se numără:

- Tabloul de comandă personalizabil, cu vizibilitate și control al aplicației bazată pe identitatea utilizatorului
- Politici unificate, configurare și raportare separată pe wireless, switching, routing, VPN, administrare adresă IP și politici de securitate.

- Modul expres conceput pentru implementarea rețelelor Wi-Fi
- Modul Enterprise Advanced destinat organizațiilor mari cu solicitări de politici sofisticate
- Planificator integrat, Captură de pachete, instrumente pentru urmărirea clientului pentru a facilita implementarea și depanarea la distanță
- Analiza spectrului pentru a detecta și identifica surse de interferență non-WiFi în benzile 2,4 GHz și 5 GHz;
- Sistem de raportare a dispozitivelor clienților și a sistemelor de operare
- Raportarea dispozitivelor clienților și a sistemelor de operare în funcție de utilizare, tendințe SSID și distribuția clienților pe dispozitive.
- Aplicație web cu o interfață robustă disponibilă pe Windows, Linux sau MAC OS X cu funcții avansate, cum ar fi implementarea cu configurație zero, gestionarea integrată a adreselor IP ce oferă o administrare unificată, monitorizare și vizibilitate la distanță pentru toate dispozitivele dvs.

11. SLA și Procedura de raportare a defecţiunilor

11.1. SLA – Service Level Agreement

11.1.1. Mod de calcul SLA

Disponibilitate / lună = ((Timp total de disponibilitate pe lună)* – (Suma timpului de indisponibilitate)) / (Timp total de disponibilitate pe lună) x 100

Timpul total de disponibilitate pe lună = numărul total de minute pe lună pentru care serviciul trebuie să fie funcțional

Suma timpului de indisponibilitate = numărul de minute în care serviciul este complet nefuncțional

*În situația în care durata serviciului este mai mică de o lună, se va lua în considerare termenul fracționat;

La determinarea timpului de indisponibilitate, nu se vor lua în calcul perioadele de indisponibilitate a Serviciului determinate de cauze care nu pot fi imputabile Furnizorului, inclusiv orice disfuncționalități ale sistemelor si serviciilor operationale proprii ale Clientului sau furnizate de terti. Indicăm cu titlu de exemplu, lipsa accesului la serviciul de internet proprietate Client furnizat de un terț, disfuncționalități și întreruperi în furnizarea altor servicii de către terți - energie electrică etc.

11.1.2. Serviciul CPE-A, IACC, VPN, CCS-E, CCS-A

Disponibilitate garantata: 99.5%, în caz contrar Clientul putând solicita penalități conform grilei de mai jos, fără ca suma totală a penalităților să poată depăși 100% din tariful lunar al serviciului.

Între 99.5% - 98.0%	5% din tariful lunar al serviciului
Între 98.0% - 97.0%	10% din tariful lunar al serviciului
Între 97.0% - 96.0%	15% din tariful lunar al serviciului
Mai puţin de 96%	20% din tariful lunar al serviciului

11.1.3. Serviciul VPS-E, VPS-A, VPS-S

Disponibilitate garantata: 99.9%, în caz contrar Clientul putând solicita penalități conform grilei de mai jos, fără ca suma totală a penalităților să poată depăși 100% din tariful lunar al serviciului.

Între 99.9% - 98.0%	5% din tariful lunar al serviciului
Între 98.0% - 97.0%	10% din tariful lunar al serviciului
Între 97.0% - 96.0%	15% din tariful lunar al serviciului
Mai puţin de 96%	20% din tariful lunar al serviciului

11.2. Procedura de raportare a defecţiunilor

Un raport de defecţiune emis de Beneficiar trebuie să includă următoarele:

- numele și datele de contact ale client, inclusiv numărul de telefon a persoanei care a raportat defecţiunea
- Adresa sau locaţia unde defecţiunea s-a produs
- Numele şi numărul de telefon al persoanei care răspunde de locaţia indicată
- Tipul defecţiunii

Persoana care a raportat defecţiunea va primi un număr de tichet de reclamație (TT) pentru referinţe ulterioare.

1) Indisponibilitatea serviciului trebuie confirmată sau negată după procedurile de testare. Confirmarea/negarea trebuie făcută prin mesaje E-mail sau fax completate cu numele persoanei care a efectuat testele.

2) În cazul problemelor de ordin tehnic, Clientul trebuie să-şi informeze Furnizorul cu privire la plângere, trebuie să colaboreze pentru localizarea şi identificarea întreruperii serviciului şi pentru restabilirea acestuia.

Observaţie:

Toate formularele de confirmare trebuiesc să conţină o dată de începere şi una de terminare a perioadei deranjamentului, a locului defecţiunii, a cauzei defecţiunii şi soluţia pentru restabilirea serviciului.

Incidentele se raportează telefonic sau pe e- mail către următoarele puncte de contact:

Helpdesk Non-Stop COMBRIDGE:

a. telefonic, la numerele: +40.31.080.0000 / +40.751.291.695
b. prin email, la adresa: support@combridge.ro zilnic, 24/7 h

Informațiile necesare deschiderii tichetului (nota de incident):

- Persoana de contact;
- Descrierea detaliată a defecțiunii;
- Număr de telefon;
- Data/ora de începere a defecțiunii;
- Detalii serviciu (detaliile tehnice primite la punerea în funcţiune a serviciului);

Confirmarea tichetului are loc prin e-mail.

După verificarea aspectelor reclamate, echipa de suport Combridge va transmite un răspuns clientului, în termen de 1 (o) ora de la primirea reclamației. Răspunsul va consta în informaţii despre natura defecţiunii şi timpul de remediere.
Timpul de remediere va fi stabilit în funcţie de natura defecţiunii, şi poate dura până la 4 (patru) ore.

Ierahia de escaladare, în condițiile în care Beneficiarul nu este satisfăcut de modul în care incidentul este rezolvat:

Level 1 :			
Department Phone 1 Phone 2 Fax Mobile E-Mail	**Helpdesk** +4031 0800 000 +4021 3120 396 +4031 0800 201 +40751291 695 support@combridge.ro	24/7/365	În timpul orelor de program Între 09:00 şi 18.00
Level 2			
  Phone Fax Mobile E-Mail	**Gabriel Chifu** Helpdesk – Team Leader +4031 0800 001 +40 31 0800 201 +40784277451 gabriel.chifu@combridge.ro	Luni-Vineri	În timpul orelor de program Între 09:00 şi 18.00
Level 3			
  Phone Fax Mobile E-Mail	**Razvan Bogdan** Technical Manager Network Engineering +40 31 0800 229 +40 31 0800 201 +40751265553 razvan.bogdan@combridge.ro	Luni-Vineri	În timpul orelor de program Între 09:00 şi 18.00
Level 4			
  Phone Fax Mobile E-Mail	**Adrian Rosu** Technical Director +40 31 0800 218 +40 31 0800 201 +40 748 039 008 adrian.rosu@combridge.ro	Luni-Vineri	În timpul orelor de program Între 09:00 şi 18.00
Level 5			
  Phone Fax Mobil RO E-Mail	**Endre Magyari** Business Development Director +40 31 0800 202 +40 31 0800 201 +40 744 794 735 magyari.endre@combridge.ro	Luni-Vineri	În timpul orelor de program Între 09:00 şi 18.00

Documentul Anexa nr.1 Specificatii tehnice ale produselor si Serviciilor Combridge este semnat pentru conformitate de catre reprezentantul legal al S.C.Combridge SRL, dl. Csenteri Andras Levente – Director executiv.