Internet
pre firmy

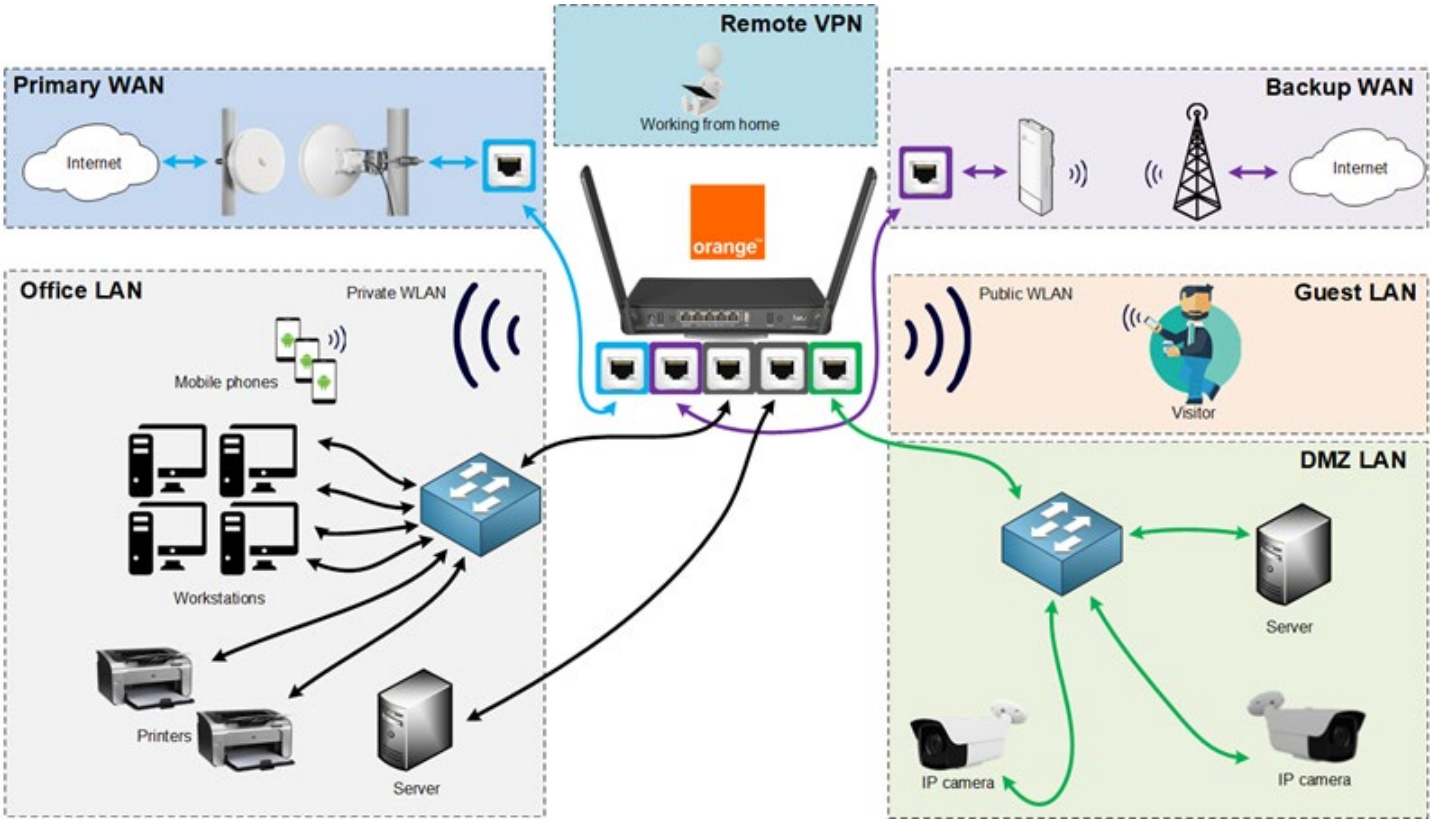
orange™

Obsah

Úvod

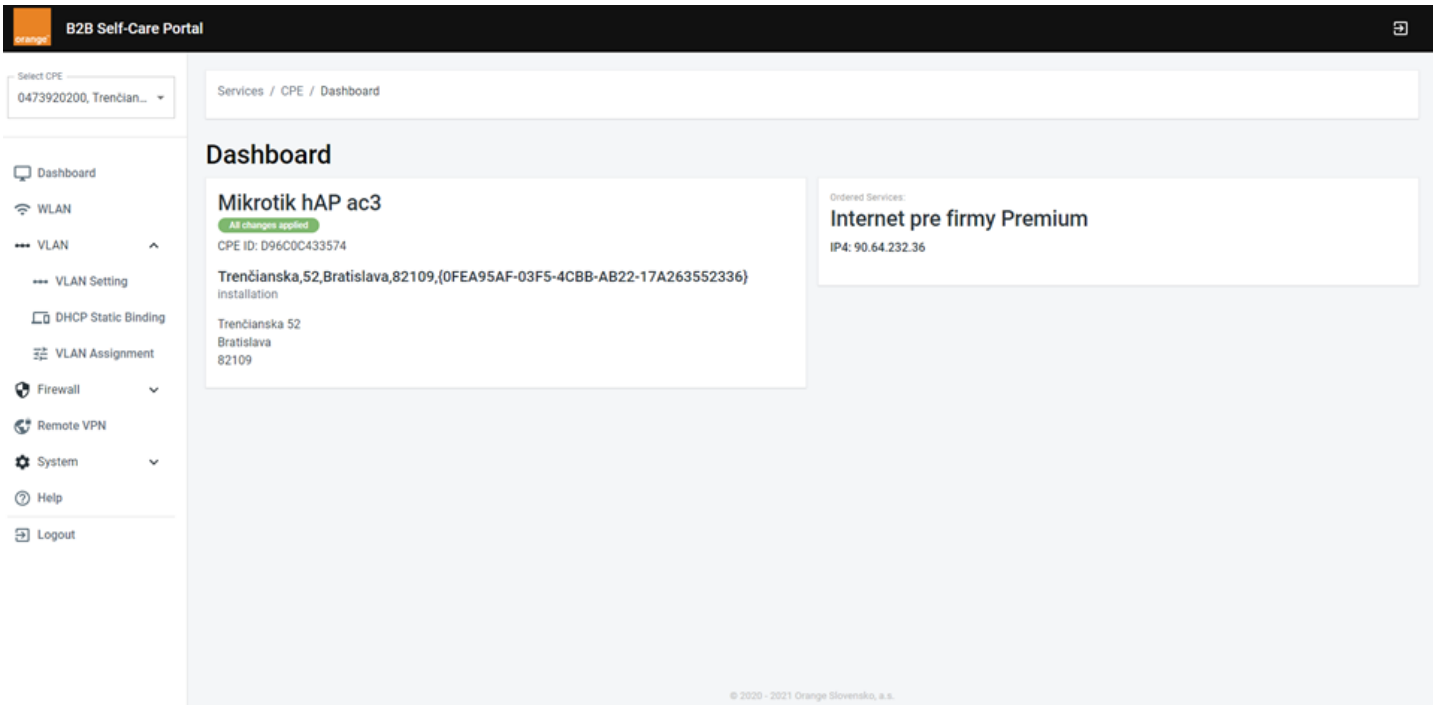
Internet pre firmy je služba, ktorá nám v prvom rade zabezpečuje pripojenie do internetu pomocou rôznych prístupových technológií, ako sú 60GHz technológia, LTE, xDSL, optika a v budúcnosti aj iné. V rámci služby dostávame statickú verejnú IPv4 adresu, tri preddefinované LAN segmenty (VLANy), výkonnú Dual Band Wi-Fi so štyrmi preddefinovanými SSID. Máme možnosť si vytvárať rôzne firewall pravidlá, presmerovania portov, statické DHCP bindingy a iné. Veľkou výhodou služby je možnosť zapnutia VPN servera (Remote VPN), vďaka čomu získavame prístup do lokálnej siete odvšadiaľ. Všetky možnosti nastavenia služby sú predstavené v nasledujúcich kapitolách. Z doplnkových služieb máme možnosť si aktivovať IPv4 rozsah (/29) namiesto jednej IPv4 adresy, DDoS ochranu a záložné pripojenie do internetu – backup WAN (automatický failover a failback), SLA plus.

Máme na výber z dvoch prenajímaných zariadení. Prvý router je menej výkonný avšak zaujme menšou cenou. Hlavnou nevýhodou by mohli byť iba 3 použiteľné LAN porty. Ak nám táto možnosť nevyhovuje, môžeme si zvoliť výkonnejší model s 8 použiteľnými LAN portami, výkonnejším systémom a Wi-Fi. Z pohľadu ponúkaných funkcionalít sú si však routre rovnocenné.



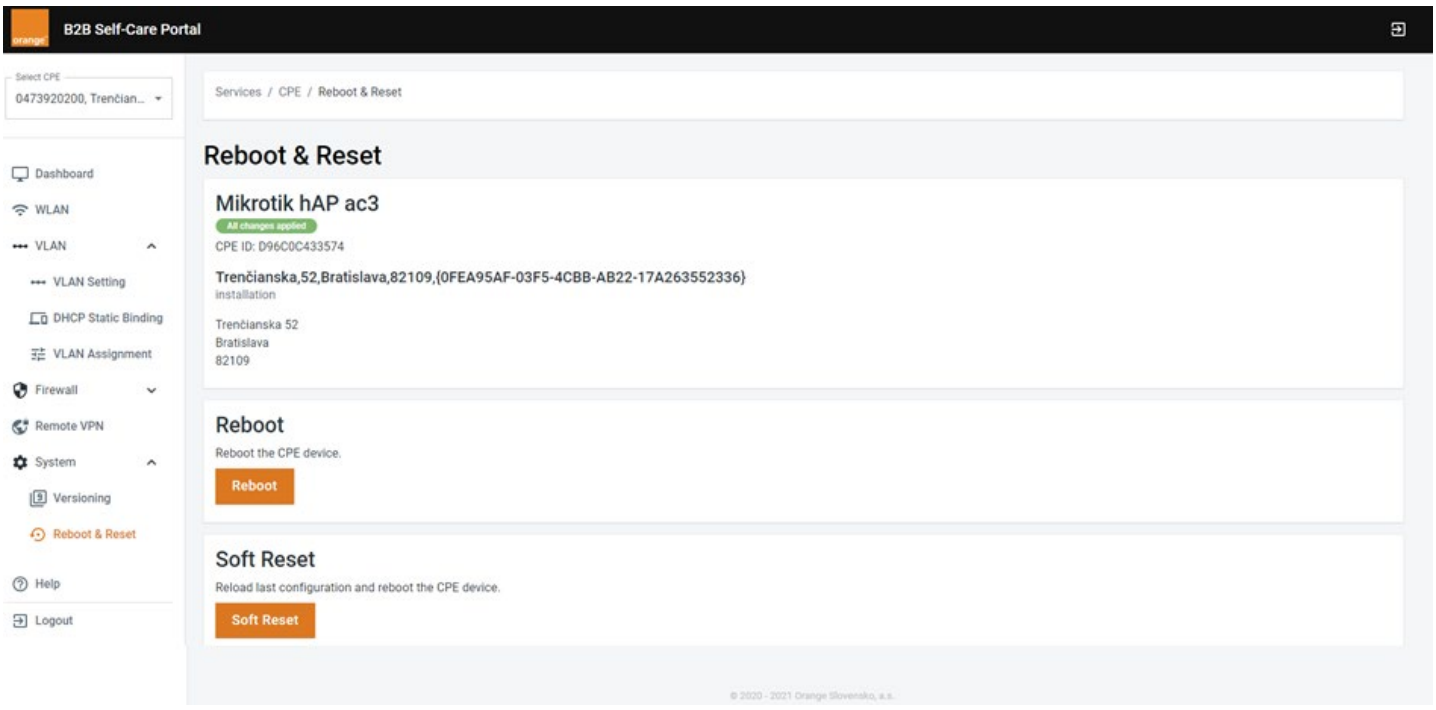
Dashboard

Dashboard je miesto, kde vidíme základné informácie o zakúpenej službe. Konkrétne tu nájdeme typ prenajatého zariadenia, jeho sériové číslo, inštalačnú adresu, priradené IP adresy/adresy a doplnkové služby. Okrem toho tu vidíme aj informáciu o tom, či konfiguračné zmeny vykonané cez portál už boli aplikované na zariadení.



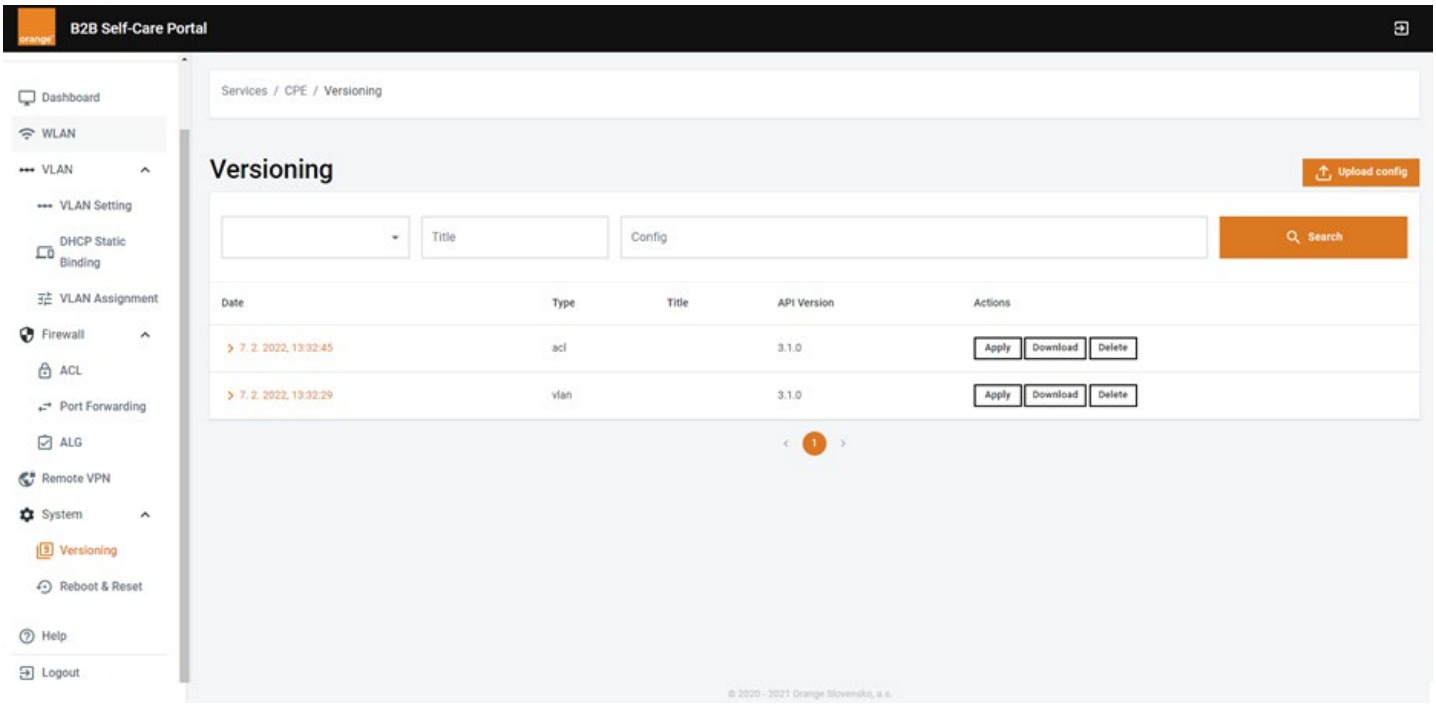
Systémové nastavenia

V systémových nastaveniach máme možnosť prenajaté zariadenie reštartnúť alebo resetnúť do továrenských nastavení. Z resetov máme na výber z dvoch možností. Soft reset nám ponechá naše nastavenia, ktoré vykonáme cez portál. Po aplikovaní továrenských nastavení sa teda dodatočne aplikujú konfiguračné zmeny z portálu. Pri hard resete sa zariadenie dostane do továrenských nastavení a ostane v stave, v akom bola služba zriadená.



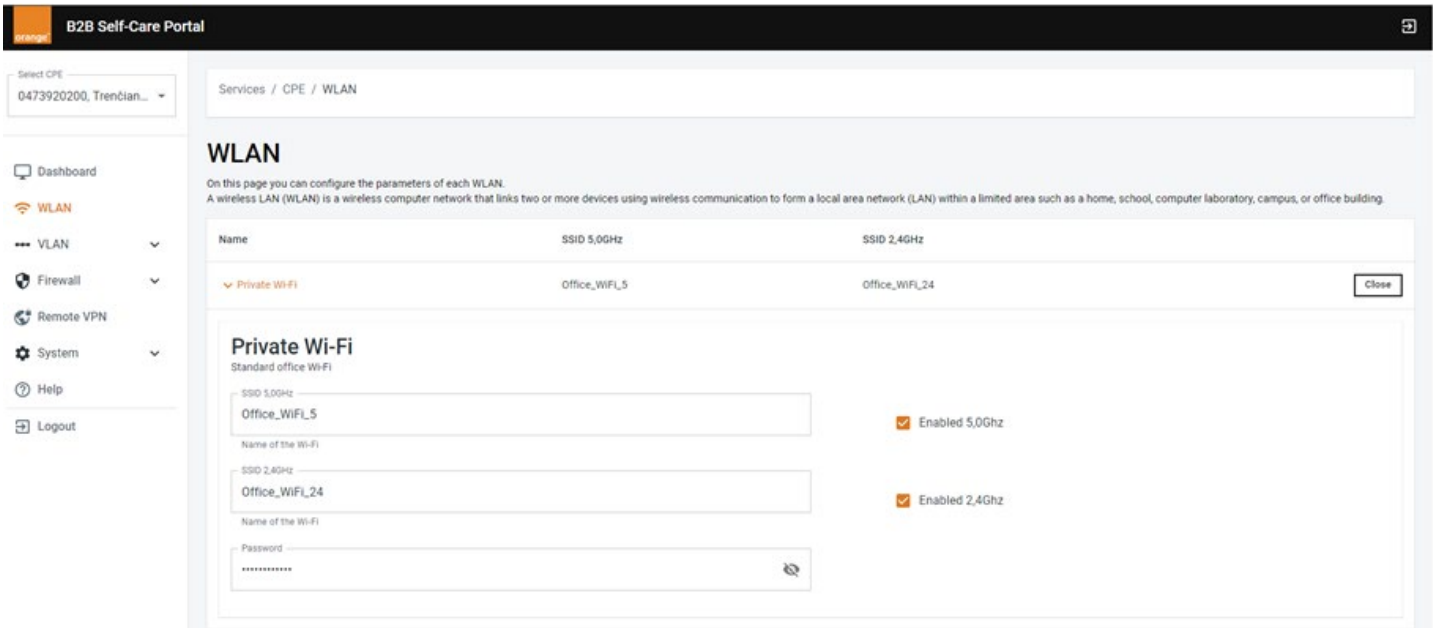
Návrat k staršej verzii konfigurácie

V systémovej sekcii sa dokážeme vrátiť k prechádzajúcim verziám konfigurácie. Tieto verzie nájdeme v sekcii „Versioning“. Každá verzia nesie časovú značku, sekciu, v ktorej bola zmena vykonaná, voliteľný popis a akcie. Verzie konfigurácie vieme aplikovať, zmazať, prípadne si ich lokálne stiahnuť.

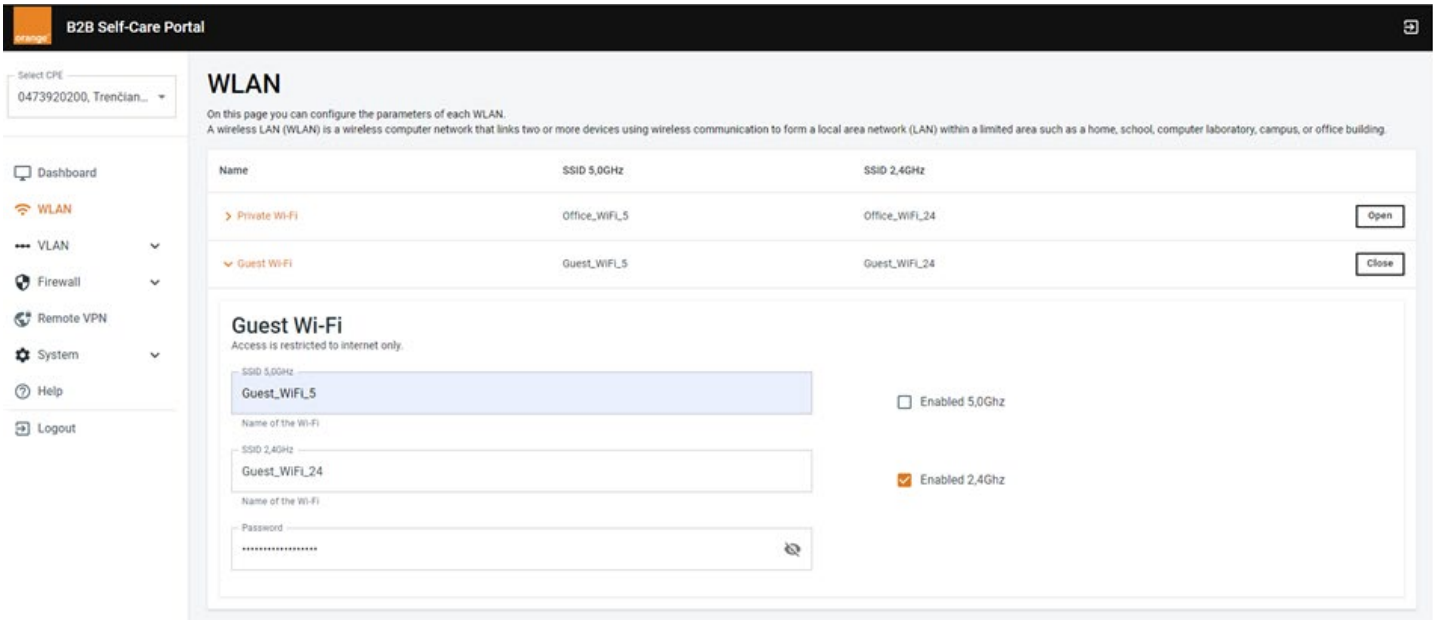


Wireless nastavenia (Wi-Fi/WLAN)

V sekcii WLAN si môžeme nastaviť bezdrôtové nastavania (Wi-Fi) pre dve VLANy. Prvá VLAN je Office LAN, v ktorej si nastavujeme privátne Wi-Fi, ktoré potrebujeme používať v rámci firmy. Druhá VLAN je Guest LAN a je určená primárne pre hostí, ktorí majú mať prístup iba na internet. Heslo je zdieľané pre obe pásma v rámci jednej VLAN. SSID (názov Wi-Fi) si môžeme zvoliť rovnaké v rámci jednej VLAN. Každú jednu Wi-Fi je možné vypnúť. Pokiaľ vypneme privátnu Wi-Fi na niektorom pásme, automaticky sa vypne aj Guest Wi-Fi na danom pásme.



Pri privátnej Wi-Fi sme si zvolili, že SSID pre jednotlivé pásma rozdelíme. Obidve Wi-Fi sme nechali zapnuté.

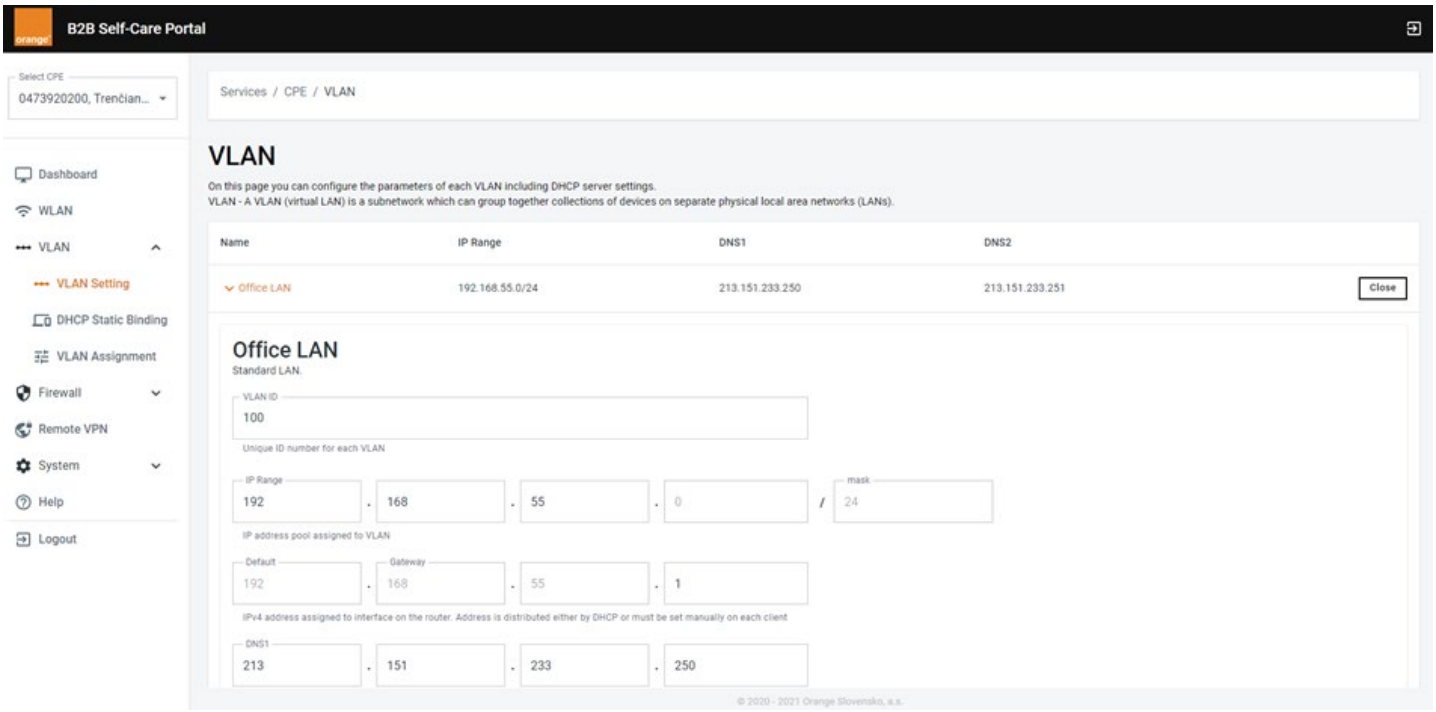


Pri hosťovskej Wi-Fi sme opäť zvolili cestu rozdielnych názvov. 5 GHz pásmo sme však vypli.

Nastavenie lokálnej siete a jednotlivých VLAN

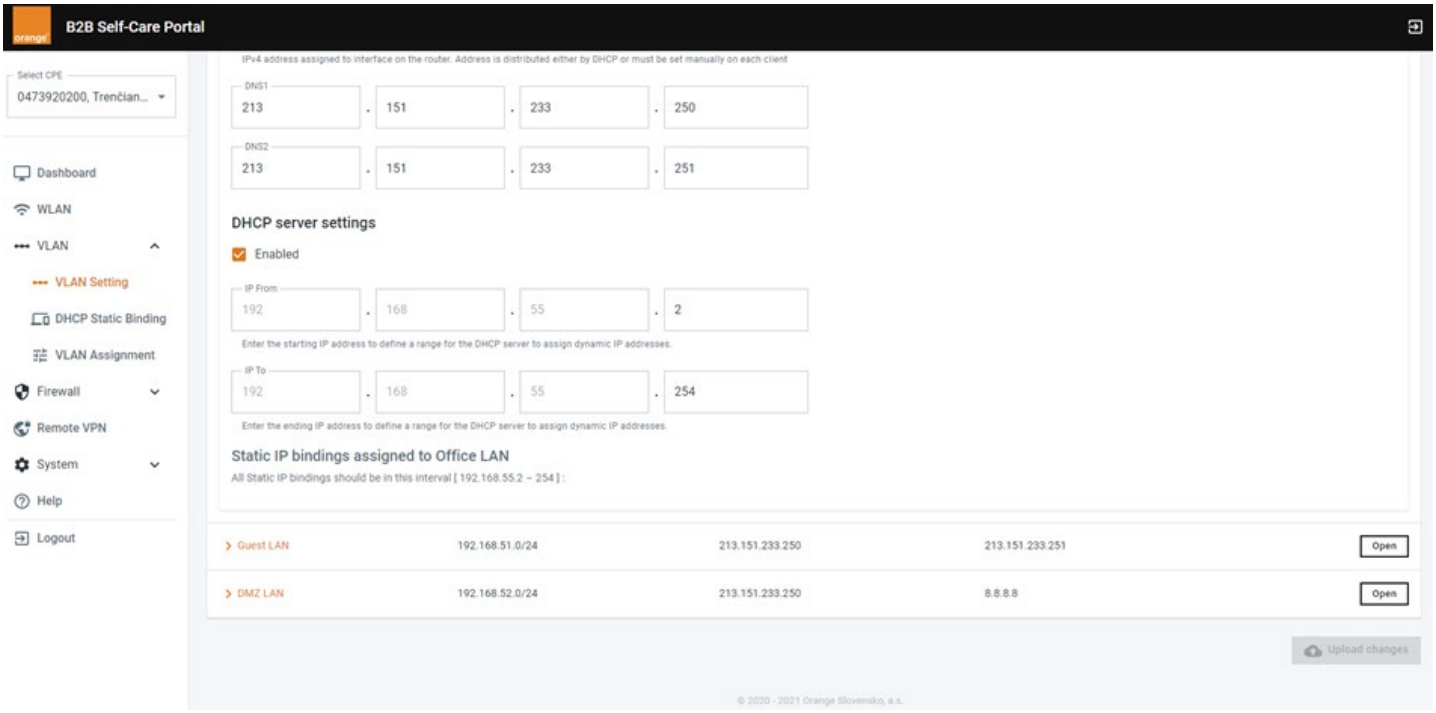
V rámci domácej siete si vieme nastaviť tri preddefinované VLANs – Office LAN, Guest LAN a DMZ LAN. Office LAN je štandardná LAN sieť pre našu firmu. Guest LAN predstavuje sieť určenú pre hostí, ktorí nemajú prístup do iných VLAN. Majú prístup iba do internetu. DMZ LAN je v základnom nastavení rovnaká ako Office LAN. Jej funkcia sa mení pri doplnkovej službe dodatočné IP adresy (viac nižšie).

Pre každú VLAN máme dostupných niekoľko nastavení.

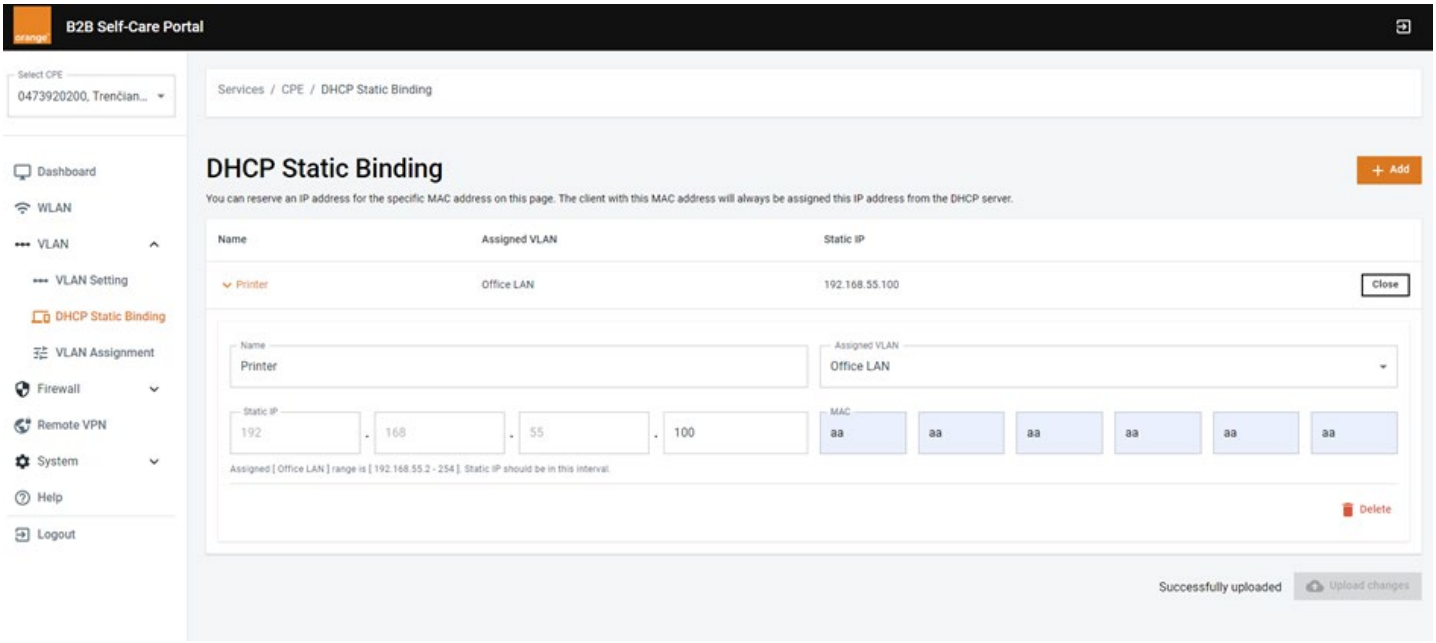


- V prvom kroku si môžeme zvoliť VLAN ID, čo je označenie VLANy. Toto nastavenie nie je potrebné meniť, pokiaľ nechceme používať TRUNK porty a prvotné nastavenie VLAN ID nám nevyhovuje.
- V ďalšom kroku si zvolíme rozsah IP adries. Niektoré adresné priestory nebude možné nastaviť, aby nevznikli konflikty IP adries. Takisto každý IP rozsah v rámci služby musí byť unikátny. Pre každú VLAN je možné použiť iba masku /24. Máme teda 253 použiteľných privátnych IP adries. Nepoužiteľné sú adresy siete .0, default gateway adresa a broadcast adresa .255.

- Nasleduje nastavenie default gateway adresy. Je to adresa, ktorú bude používať router pre danú VLAN. Táto adresa je potrebná pre každé klientske zariadenie v lokálnej sieti. Bez tohto nastavenia sa klientske zariadenie nedokáže dostať mimo lokálnej siete. Adresa default gateway musí byť mimo intervalu, ktorý nastavujeme pre DHCP server.
- Ďalej nastavujeme DNS nastavenia. DNS1 predstavuje primárny DNS server a toto nastavenie je povinné. DNS2 je voliteľné nastavenie a nie je potrebné túto položku vypĺňať.

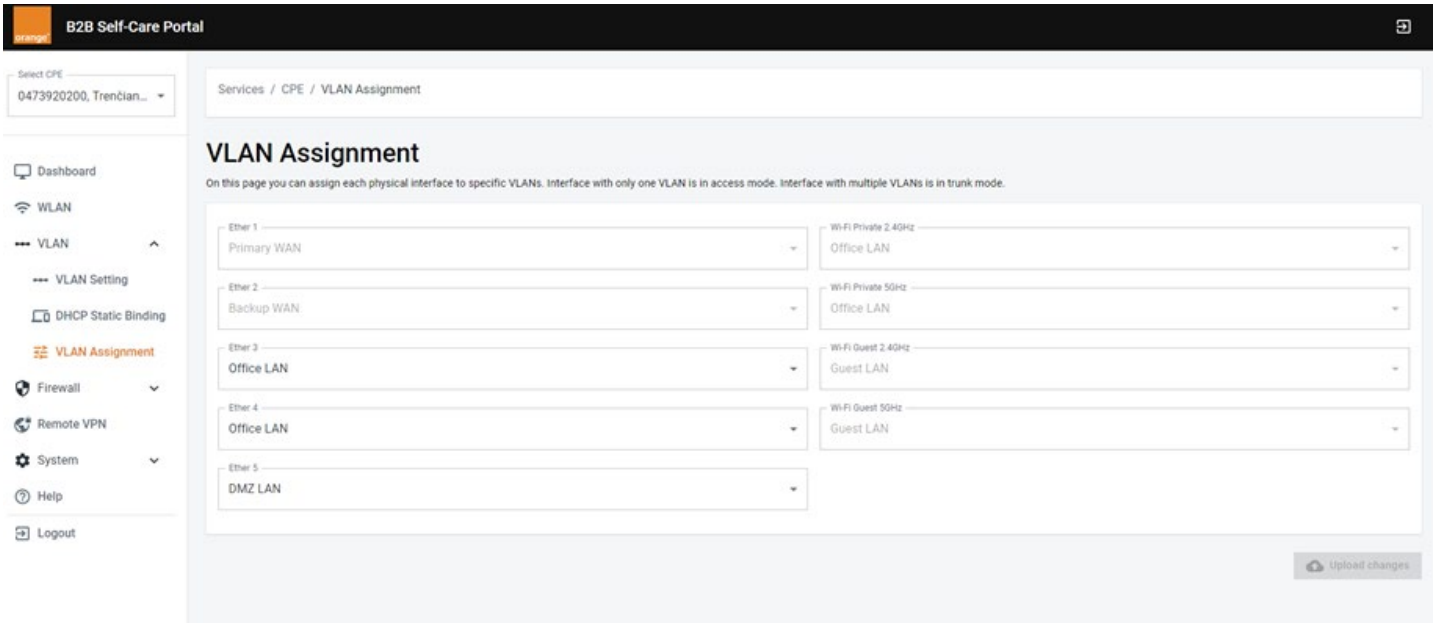


- Ďalšia sekcia nastavení súvisí s DHCP serverom pre danú VLAN. DHCP server automaticky prideľuje IP adresy klientskym zariadeniam, ktoré si pýtajú IP adresu pomocou DHCP klienta. DHCP server si vieme pre každú VLAN vypnúť. Dôležitý je aj interval IP adries, z ktorého má DHCP server adresy prideľovať. Tento interval si môžeme zmeniť napríklad z dôvodu, že si chceme nechať nejaké IP adresy na účely statických nastavení.
- V prípade, že chceme nechať prideľovanie IP adries dynamické cez DHCP server, ale zároveň potrebujeme, aby sa niektorým zariadeniam IP adresy nemenili, môžeme využiť nastavenia DHCP statických bindingov. Pri takomto nastavení si musíme zvoliť, do ktorej VLAN zariadenie patrí a potrebujeme poznať jeho MAC adresu. Bežne takéto nastavenie potrebujeme pre servery alebo tlačiarne.



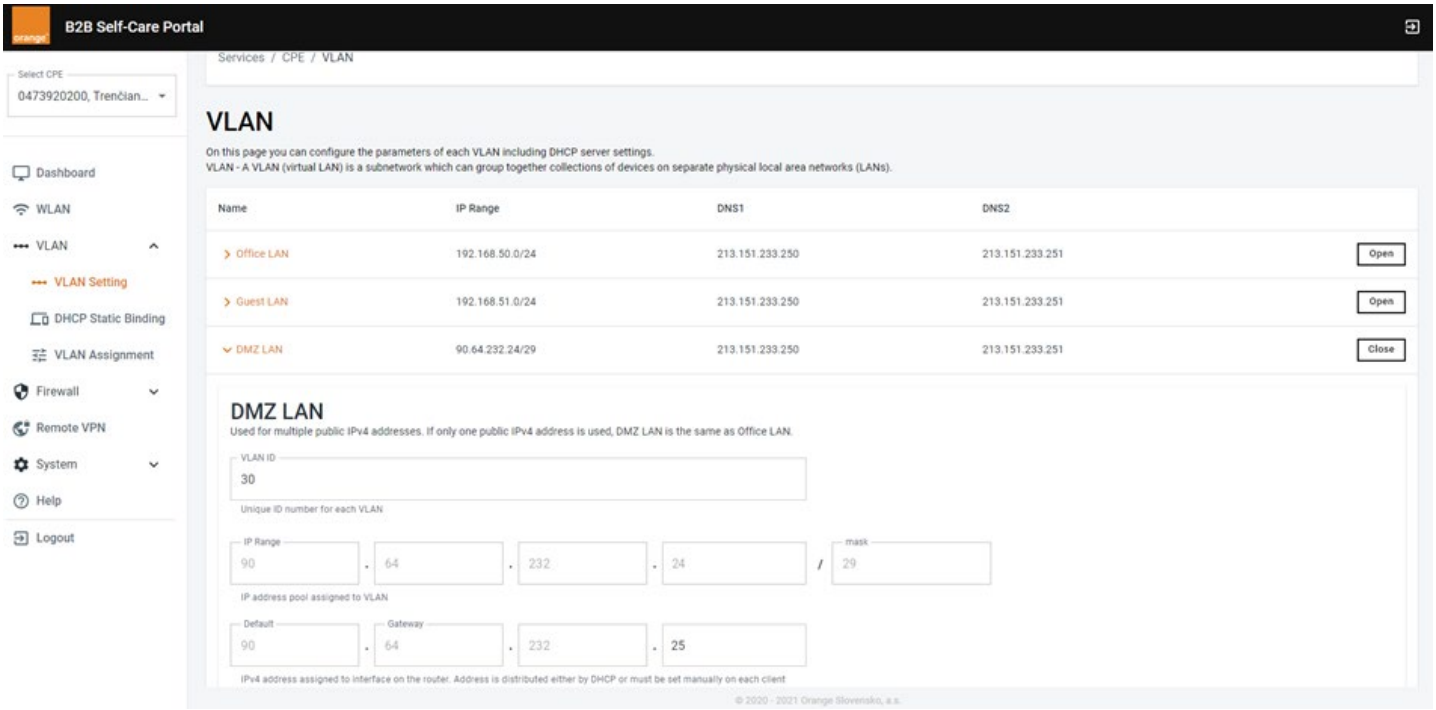
- V poslednom kroku si potrebujeme zvoliť, ktoré rozhrania budú patriť do ktorej VLAN. Tieto nastavenia nájdeme v sekcii VLAN Assignment. Rozhrania Ether 1 a Ether 2 sú vyhradené pre WAN konektivity. Rovnako si nevieme zmeniť ani priradenie Wi-Fi sietí. Zvyšné rozhrania si môžeme ľubovoľne priradiť k jednotlivým VLAN. Pokiaľ je rozhranie iba v jednej VLAN, ide o takzvaný ACCESS port. V takom prípade v klientskom nastavení nie je potrebné nič ďalšie nastavovať.

V prípade dvoch alebo troch VLAN na jednom rozhraní hovoríme o TRUNK porte. V takom prípade musíme na daný port pripojiť zariadenie, ktoré vie pracovať s TRUNK portami, ako je napríklad switch.

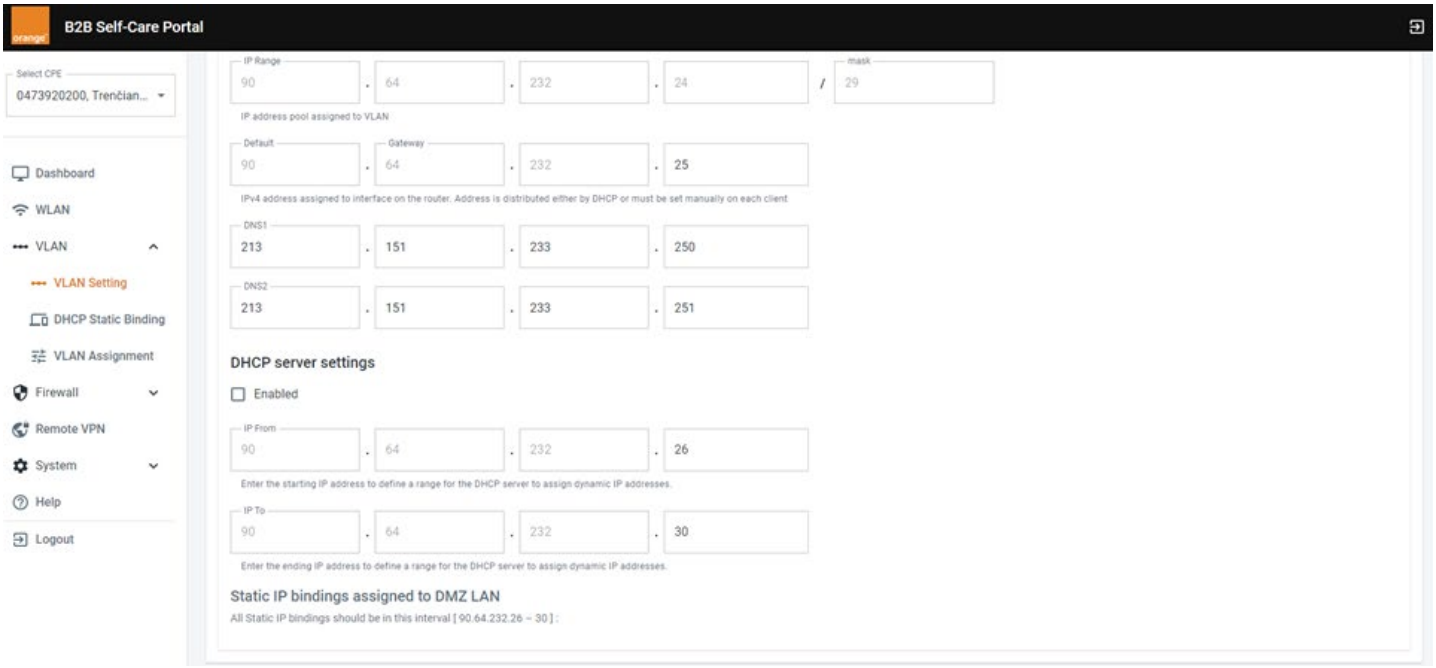


Doplnková služba dodatočné IP adresy

Ak sme si zakúpili dodatočné IP adresy, dostaneme /29 IPv4 adresný priestor, z ktorého vieme použiť 5 IP adries. V takomto prípade sa nám zmení funkcia DMZ VLAN. Práve táto VLAN dostane nastavenia zakúpeného adresného priestoru. Nebude teda možné meniť si adresný priestor pre DMZ VLAN, aby neprišlo k znefunkčneniu služby.



Stále si však môžeme zmeniť nastavenie default gateway, prípadne nastavenia DHCP servera.



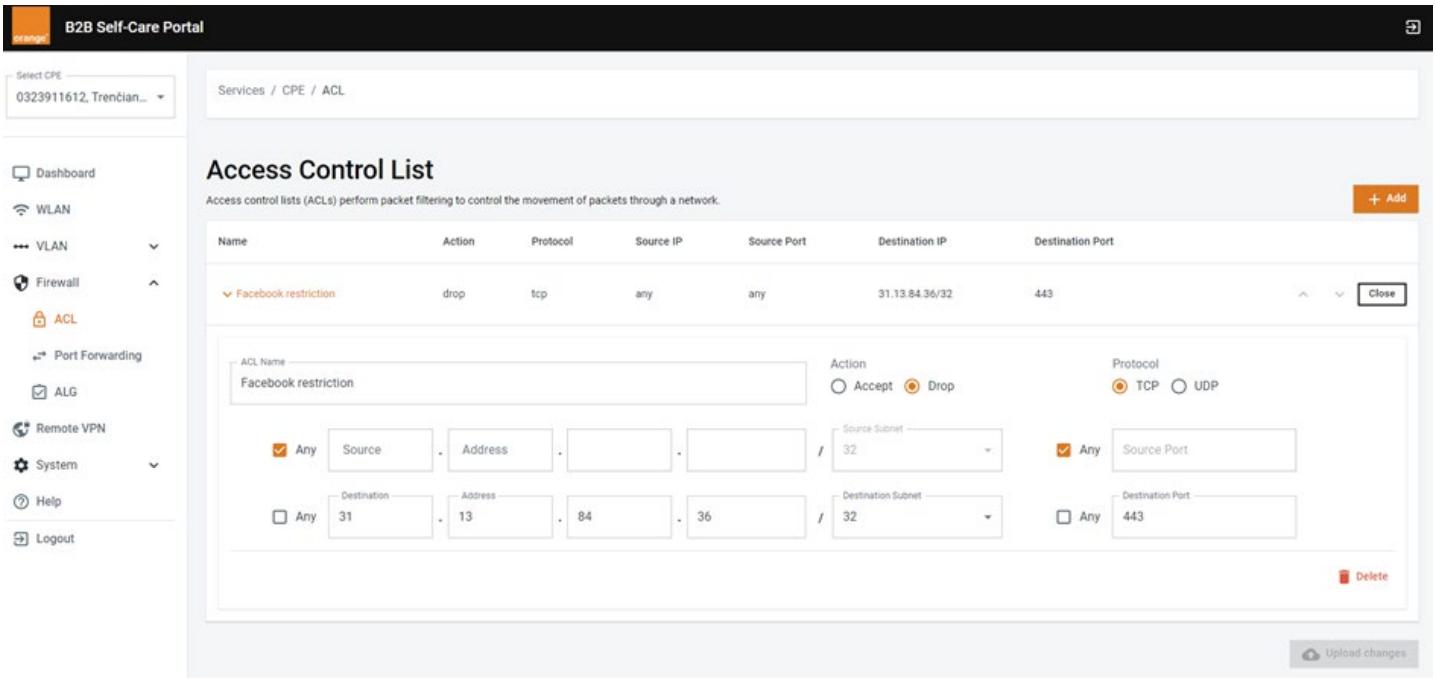
Použitie vlastného routra

Služba dodatočné IP adresy je potrebná, ak potrebujeme používať vlastný router. Prenajímané zariadenie totiž musí ostať v L3 móde, aby bol zabezpečený bezproblémový chod služieb. Vlastný router v takomto prípade zapojíme do hociktorého portu, ktorý je priradený do DMZ LAN. Podľa potreby si ponecháme zapnutý DHCP server alebo ho vypneme a IP adresy staticky nastavíme. Pokiaľ potrebujeme povoliť komunikáciu smerom na vlastný router, musíme vytvoriť adekvátne ACL pravidlo.

Nastavenie ACL (firewall)

V tejto sekcii si vieme nastaviť rôzne firewall pravidlá. Vieme si však meniť iba forward flow. Nevieme teda upravovať firewall pravidlá, keď je cieľom prenajaté zariadenie. Môžeme si napríklad nastaviť, aby z našej lokálnej siete nebol prístup na sociálnu sieť Facebook. Vo všeobecnosti je v prvotných nastaveniach služby povolená všetka komunikácia z lokálnej siete von (do internetu) a všetka komunikácia iniciovaná z vonkajšej siete (z internetu) do lokálnej siete je zakázaná. Pokiaľ si pri doplnkovej službe dodatočné IP adresy potrebujeme povoliť komunikáciu do DMZ LAN, musíme si na to vytvoriť adekvátne ACL pravidlo.

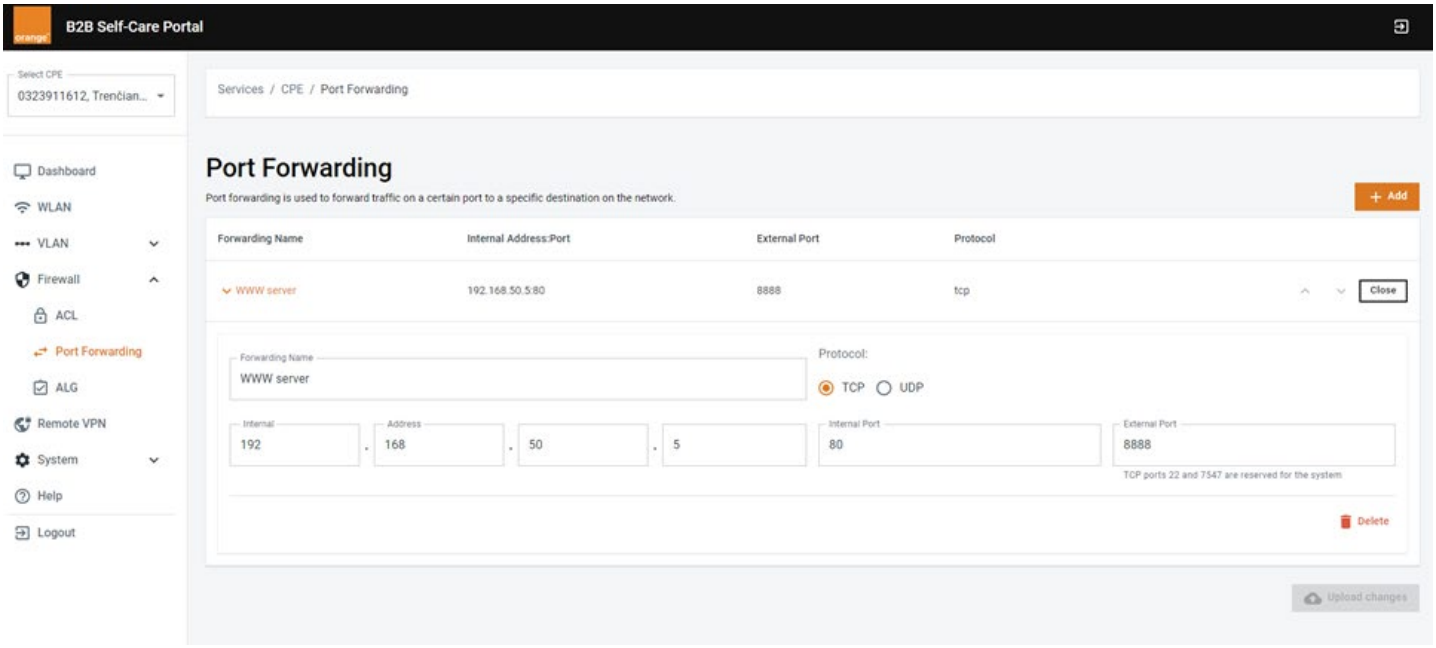
Pri každom ACL pravidle si potrebujeme zadefinovať akciu, ktorá sa má vykonať. Buď chceme komunikáciu povoliť, alebo zakázať. Ďalej si potrebujeme zvoliť buď TCP, alebo UDP protokol. Vieme, že webová komunikácia je pod TCP protokolom. V ďalšom kroku si musíme zadefinovať zdrojovú a cieľovú IP adresu/adresy pre naše pravidlo. Môžeme si zvoliť aj možnosť „Any“. V našom prípade nám táto možnosť vyhovuje, keďže chceme zakázať komunikáciu pre celú lokálnu sieť. Ako cieľovú adresu dáme adresu Facebooku. Nasleduje nastavenie aplikačných portov. Vo všeobecnosti zdrojové porty môžeme nechať na „Any“, keďže sú väčšinou náhodne generované. Cieľové porty sú však dôležité. V našom prípade potrebujeme zakázať HTTPS komunikáciu, ktorá je na porte 443.



Nastavenie port forwardingu (presmerovanie portov)

V tejto sekcii si vieme nastaviť rôzne pravidlá presmerovania portov. To znamená, že keď takáto komunikácia príde z vonkajšej siete na prenajaté zariadenie, automaticky bude presmerované na požadované klientske zariadenie a požadovaný port.

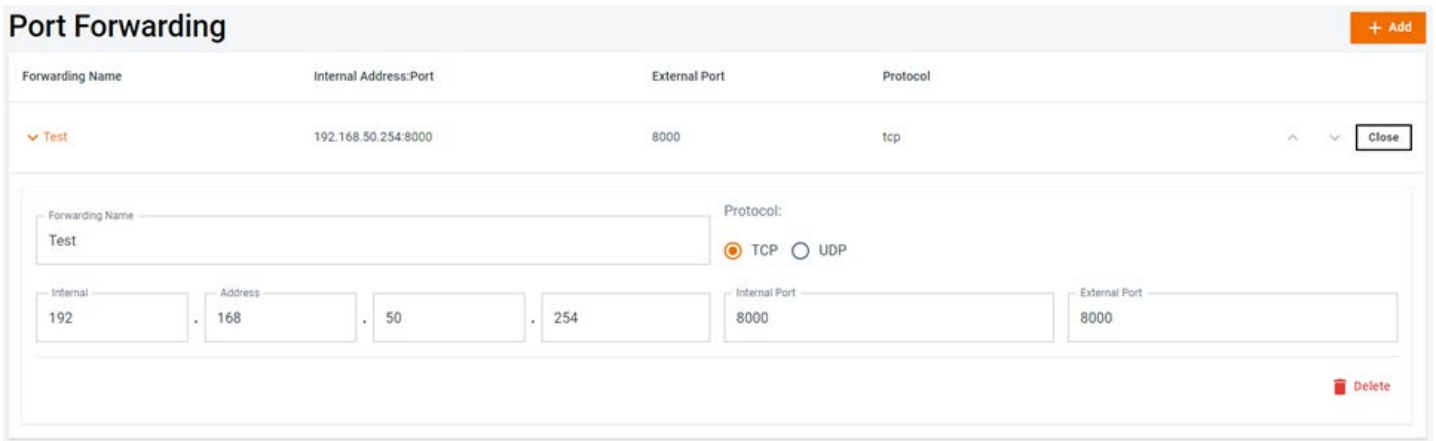
Pri každom nastavení presmerovania portov je potrebné si opäť zvoliť protokol TCP alebo UDP. Následne si zvolíme IP adresu v lokálnej sieti nášho zariadenia, kam chceme komunikáciu presmerovať. V tomto prípade sa nám hodia DHCP statické bindingy, ktoré sme si nastavili pri nastavovaní lokálnej siete. Ďalej si musíme zvoliť externý a interný port. Externý port je port, na ktorom bude počúvať prenajaté zariadenie a interný port patrí nášmu klientskemu zariadeniu.



Reštrikcia zdrojových adries pri definovaní port forwarding pravidiel

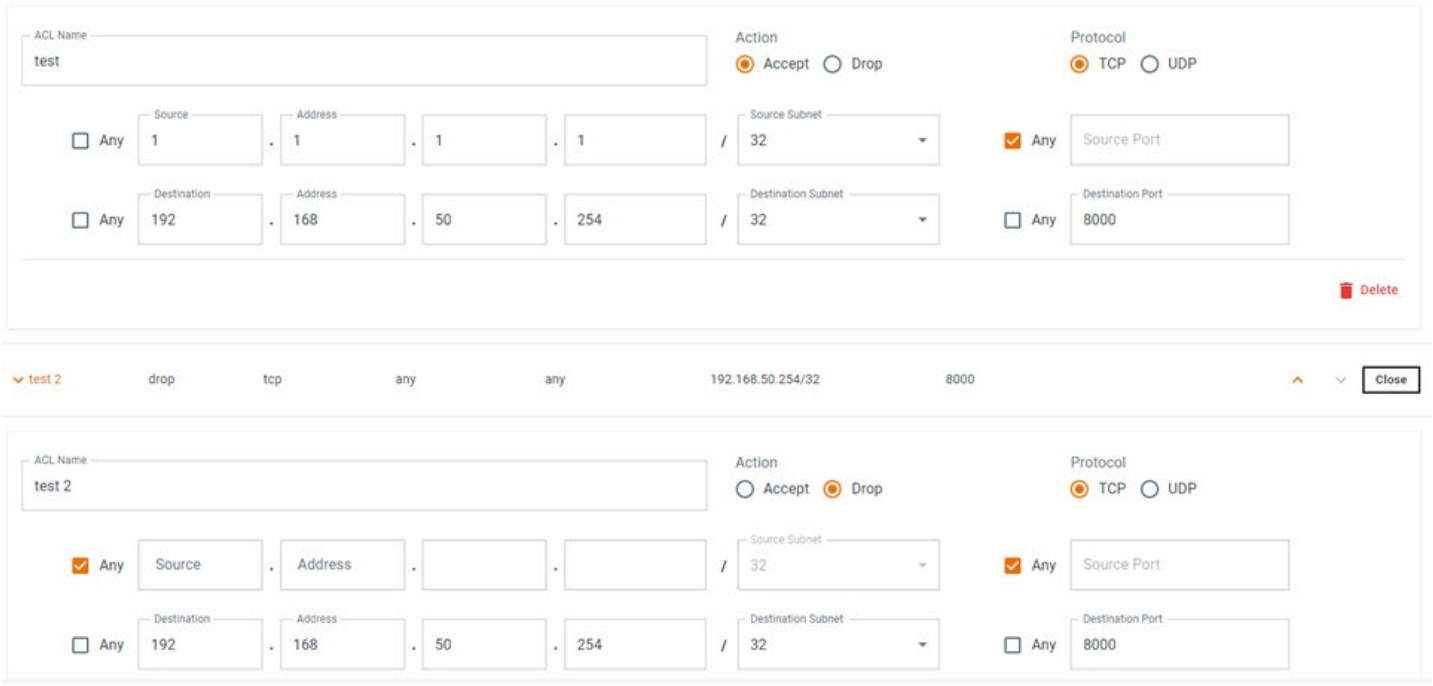
Potrebujeme si nastaviť port forwarding pre server v LAN, ktorý má IP adresu 192.168.50.254 a počúva na TCP porte 8000. Komunikáciu chceme obmedziť tak, že povolíme komunikáciu na server iba z IP adresy 1.1.1.1.

Port forwarding:



Použijeme bežné nastavenie port forwardingu. Ako internú adresu zadáme IP adresu servera 192.168.50.254. Protokol zvolíme TCP a interný port 8000. Externý port môže byť ľubovoľný okrem portov vyhradených pre systém (TCP 22 a 7547).

ACL:

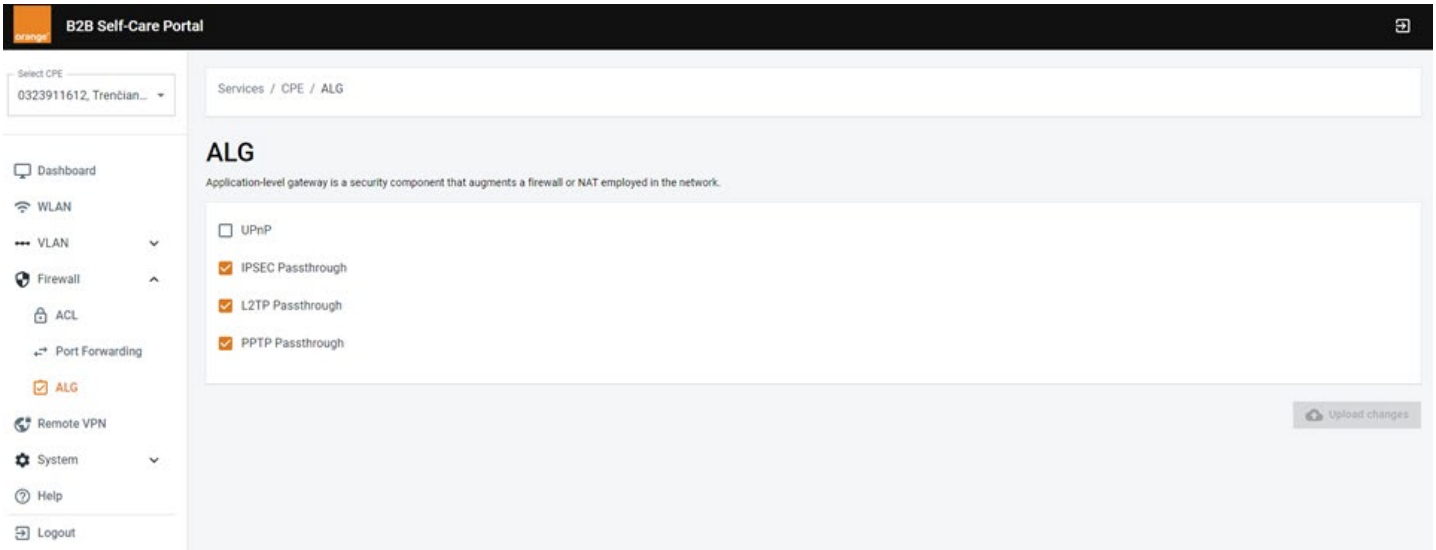


Na obmedzenie komunikácie z pohľadu source adresy je nutné nastaviť dve ACL pravidlá. V prvom pravidle povolíme komunikáciu z tých IP adries, ktoré potrebujeme. Druhé pravidlo zakáže všetku ostatnú komunikáciu smerovanú na náš server.

Počet pravidiel môže byť aj vyšší, ak potrebujeme povoliť viac source adries, ktoré nevieme zlúčiť do jedného subnetu. Posledné pravidlo je však vždy rovnaké.

Nastavenie ALG (Application Level Gateway)

ALG pravidlá sú špeciálne pravidlá firewallu, ktoré vedia napríklad povoliť priepustnosť IPSec protokolu. Z dostupných nastavení máme možnosť si zapnúť alebo vypnúť nasledovné ALG:

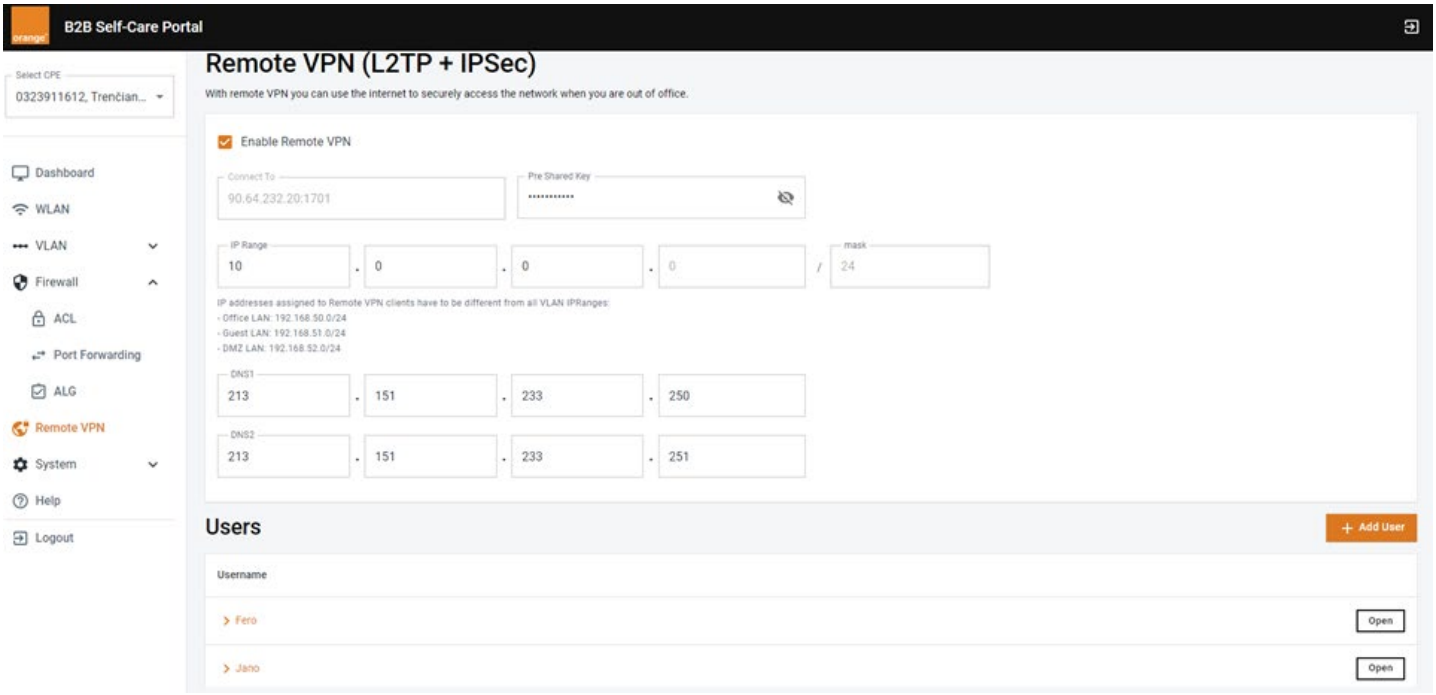


Pravidlo UPnP umožňuje dynamické vytváranie presmerovania portov, pokiaľ si o to klientske zariadenia požiadajú. Ostatné pravidlá umožňujú prepúšťanie uvedených VPN technológií. Niektoré ALG helpery ako napríklad pre FTP alebo SIP sú automaticky zapnuté.

Nastavenie Remote VPN (vzdialený prístup do lokálnej siete)

Pri tejto službe máme možnosť si jednoducho aktivovať vzdialený prístup do lokálnej siete. Tento prístup je zabezpečený pomocou L2TP + IPSec protokolu a zdieľaného hesla. Maximálny počet spojení v jednom čase je 5. Počet používateľov je ľubovoľný.

V prvom rade si musíme nastaviť zdieľané heslo v poli „Pre Shared Key“. Ďalej si nastavíme IP rozsah, ktorý bude prideľovaný klientom Remote VPN. Platia rovnaké pravidlá ako pri lokálnej sieti, že IP rozsah musí byť unikátny a DNS2 je voliteľný. Ďalej si musíme zadefinovať používateľov, ktorí sa budú môcť hlásiť do Remote VPN.



Nakonfigurujte a používajte L2TP v systéme Windows 10

Na vytvorenie pripojenia L2TP VPN môžete použiť klienta Windows 10 VPN.

Nakonfigurujte pripojenie L2TP

Ak chcete pripraviť počítač so systémom Windows 10 na vytvorenie pripojenia L2TP VPN, musíte nakonfigurovať pripojenie L2TP v nastaveniach siete.

1. V ponuke Štart systému Windows 10 kliknite na položku **Settings**.
2. Kliknite na položku **Network & Internet**.
3. V ľavej navigačnej ponuke vyberte **VPN**.
4. Kliknite na **Add a VPN** connection.
5. V textovom poli **VPN provider** vyberte **Windows (built-in)**.
6. Do textového poľa **Connection name** zadajte názov siete VPN (napríklad „L2TP VPN“).
7. Do textového poľa **Server name or address** zadajte názov DNS alebo IP adresu servera VPN.
8. V rozbaľovacom zozname **VPN Type** vyberte protokol **Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)**.
9. Kliknite na tlačidlo **Save**.
   Sieť VPN sa pridá na stránku nastavení siete a internetu VPN.
10. Na stránke nastavení VPN kliknite na **Change adapter options**.
11. Kliknite na svoju VPN a vyberte ju.
12. Kliknite na položku **Change setting of this connection**.
    Zobrazia sa vlastnosti pre túto sieť VPN.
13. Kliknite na kartu **Security**.
14. V rozbaľovacom zozname **Data encryption** vyberte možnosť **Require encryption (disconnect if server declines)**.
15. Vyberte možnosť **Allow these protocols**.
16. Vyberte **Microsoft CHAP Version 2** ako jediný povolený protokol.
17. Kliknite na položku **Advanced settings**.
    Zobrazí sa dialógové okno Advanced properties.
18. Vyberte **Use pre-shared key for authentication**.
19. Do textového poľa **Key** zadajte pre-shared key pre tento tunel. Pre-shared key sa musí zhodovať s pre-shared key nakonfigurovaným na routeri v nastaveniach vzdialenej siete VPN.
20. Kliknite na tlačidlo **OK**.
21. Nemeňte predvolené nastavenia na karte **Networking**.
22. Kliknite na tlačidlo **OK**.

Spustite pripojenie L2TP

Názov pripojenia VPN je názov cieľa, ktorý ste použili pri konfigurácii pripojenia L2TP na klientskom počítači. Používateľské meno a heslo odkazuje na jedného z používateľov, ktorých ste pridali do skupiny L2TP-Users.

Skôr ako začnete, skontrolujte, či má klientsky počítač aktívne pripojenie na internet.

1. V oblasti oznámení systému Windows (System tray) kliknite na ikonu **Network**.
2. Kliknite na pripojenie VPN.
3. Vyberte pripojenie VPN. Kliknite na **Connect**.
4. Zobrazí sa stránka **Connect**.
5. Zadajte svoje používateľské meno a heslo.
6. Kliknite na tlačidlo **OK**.

Nakonfigurujte a používajte L2TP v systéme macOS

macOS obsahuje natívneho klienta VPN. Klienta macOS VPN môžete použiť na vytvorenie L2TP VPN pripojenia.

Nakonfigurujte nastavenia siete L2TP

Ak chcete pripraviť zariadenie macOS na vytvorenie pripojenia L2TP VPN, musíte nakonfigurovať pripojenie L2TP v nastaveniach siete.s.

1. V ponuke Apple vyberte položku **System Preferences**.
2. Kliknite na ikonu **Network**.
3. Kliknutím na ikonu „+“ v ľavom dolnom rohu vytvorte nové sieťové rozhranie.
4. V rozbaľovacom zozname **Interface** vyberte položku **VPN**.
5. V rozbaľovacom zozname **VPN Type** vyberte **L2TP over IPSec**.
6. Do textového poľa **Service Name** zadajte názov tohto pripojenia **VPN**.
7. Kliknite na **Create**.

Môžete použiť predvolenú konfiguráciu alebo si môžete vytvoriť vlastnú konfiguráciu. Tieto kroky používajú predvolenú konfiguráciu.

8. Do textového poľa **Server Address** zadajte externú adresu IP servera VPN.
9. Do textového poľa **Account name** zadajte svoje používateľské meno.
10. Kliknite na položku **Authentication Settings**.
11. Do textového poľa **Pasword** zadajte heslo používateľa.
12. Vyberte položku **Shared Secret**.
13. Do textového poľa **Shared Secret** zadajte pre-shared key pre tento tunel. Pre-shared key sa musí zhodovať s pre-shared key nakonfigurovaným na routeri v nastaveniach vzdialenej siete VPN.
14. Kliknutím na tlačidlo **Apply** uložíte zmeny konfigurácie.

Spustite pripojenie L2TP

Názov pripojenia VPN je názov služby, ktorý ste použili pri konfigurácii pripojenia L2TP na klientskom počítači. Používateľské meno a heslo sú pre jedného z používateľov, ktorých ste pridali do skupiny L2TP používatelia.

Ak chcete spustiť pripojenie L2TP:

1. V ponuke Apple vyberte položku **System Preferences**.
2. Kliknite na ikonu **Network**.
3. Vyberte pripojenie VPN, ktoré ste vytvorili v dialógovom okne **Network**.
4. Kliknite na **Connect**.

Nakonfigurujte a používajte L2TP v systéme iOS

Zariadenia Apple iOS obsahujú natívneho klienta VPN. Tohto klienta môžete použiť na vytvorenie pripojenia L2TP VPN.

Nakonfigurujte nastavenia siete L2TP

Ak chcete nakonfigurovať pripojenie L2TP na zariadení so systémom iOS:

1. Vyberte **Settings > General > VPN**.
2. Klepnite na **Add VPN Configuration**.
3. V ponuke **Type** klepnite na **L2TP**.
4. Klepnite na **Back**.
5. Do textového poľa **Description** zadajte názov pripojenia VPN.
6. Do textového poľa **Server** zadajte externú IP adresu Fireboxu, ku ktorému sa chcete pripojiť.
7. Do textového poľa **Account** zadajte svoje meno používateľa tak, ako sa zobrazuje na autentifikačnom serveri, ktorý používate pre mobilnú sieť VPN s autentifikáciou používateľa L2TP.
8. Nechajte posúvač **RSA SecurID** vypnutý.
9. Do textového poľa **Password** zadajte heslo používateľa.
10. Do textového poľa **Secret** zadajte pre-shared key pre tento tunel. Pre-shared key sa musí zhodovať s pre-shared key nakonfigurovaným na Firebox Mobile VPN s nastaveniami L2TP IPSec.
11. Nechajte posúvač **Send All Traffic** zapnutý.
12. Ponechajte nastavenie **Proxy** vypnuté.
13. Klepnite na **Done**.

Spustite pripojenie L2TP

V tomto postupe je názvom pripojenia VPN názov služby, ktorý ste použili pri konfigurácii pripojenia L2TP na klientskom počítači.

Ak chcete spustiť pripojenie L2TP:

1. Na iOS zariadení vyberte **Settings > General > VPN**.
2. Vyberte profil L2TP VPN, ktorý chcete použiť.
3. Potiahnite **Status** to **Connecting**.

Nakonfigurujte a používajte L2TP v systéme Android

Zariadenia so systémom Android obsahujú natívneho klienta VPN. Tohto klienta môžete použiť na vytvorenie pripojenia L2TP VPN.

Nakonfigurujte nastavenia siete L2TP

Ak chcete nakonfigurovať nastavenia siete L2TP, na zariadení so systémom Android:

1. Na stránke **Settings** v časti **Wireless & Networks** vyberte položku **More > VPN**.
2. Kliknutím na + pridáte sieť VPN.
3. Do textového poľa **Name** zadajte názov tohto pripojenia VPN, napríklad „L2TP Firebox“.
4. Ak je mobilná sieť VPN s L2TP na Firebox nakonfigurovaná tak, aby používala pre-shared key ako metódu overenia IPSec:
   - v rozbaľovacom zozname **Type** vyberte **L2TP/IPSec PSK**,
   - do textového poľa **IPSec pre-shared key** zadajte pre-shared key pre tento tunel. Pre-shared key sa musí zhodovať s pre-shared key nakonfigurovaným na Firebox Mobile VPN s nastaveniami L2TP IPSec.
5. Ak je mobilná VPN s L2TP na Firebox nakonfigurovaná na používanie certifikátu ako metódy overenia IPSec:
   - v rozbaľovacom zozname **Type** vyberte **L2TP/IPSec RSA**,
   - uistite sa, že certifikát je importovaný do vášho zariadenia so systémom Android.
6. Do textového poľa **Server Address** zadajte externú adresu IP Fireboxu, ku ktorému sa chcete pripojiť.
7. Uložte pripojenie.

Spustite pripojenie L2TP

Ak chcete spustiť pripojenie VPN:

1. Vyberte L2TP VPN pripojenie, ktoré ste nakonfigurovali.
2. Zadajte svoje používateľské meno a heslo.
3. Kliknite na **Connect**.