**Управління освіти і науки Вінницької обласної державної адміністрації**
**Департамент освіти Вінницької міської ради**
**Лабораторія інформаційних та комунікаційних технологій фізико-математичної гімназії №17 м. Вінниці**

**Д.Долюк Ю.Пасіхов**

# Методичні рекомендації з розбудови локальної мережі та використання одного каналу ADSL для організації доступу в Інтернет всіх комп'ютерів мережі закладу

**Частина 3.**

**м. Вінниця**
**2011 р.**

## 1. Постановка задачі

Вважатимемо, що ми маємо мережу навчального закладу, збудовану за рекомендаціями, що викладено в ч.1 даної інструкції. Це означає, що у вас до одного ADSL-модема, налаштованого в режимі роутера, під'єднана вся локальна мережа закладу. Дане технічне вирішення дозволяє мати доступ до Інтернету з усіх ПК, але має суттєві недоліки:

- відсутність можливості організації «справедливого використання» пропускної здатності каналу;
- відсутність можливості використання в мережі будь-яких власних мережних сервісів;
- відсутність централізованих можливостей моніторингу спожитого трафіка;
- відсутність централізованої можливості фільтрації небажаних ресурсів.

***Останній недолік є вельми суттєвим в світлі вимог до обмеження доступу з навчальних комп'ютерів до шкідливого та небезпечного Інтернет-контенту.***

Ці (та багато інших) проблеми можливо вирішити, встановивши в мережі один додатковий комп'ютер з функціями маршрутизатора –шлюза (роутера) та сервера локальної мережі. Це можливо зробити з використанням серверних платформ Microsoft та спеціальних програм під ОС Windows, **але супроводжується необхідністю придбання вельми недешевих ліцензій,** потужного комп'ютера і має певні складнощі в налаштуванні. Значно дешевше (і, як показує досвід, надійніше) використовувати в якості програмної платформи для організації роутера та сервера локальної мережі ОС Linux. В частині 2 даної інструкції надавалися рекомендації по облаштуванню програмного роутера на основі базового дистрибутива Linux. Це вимагало багато «ручної» роботи та чималих знань від системного адміністратора. Найскладнішою в умовах школи була необхідність управління роутером в режимі командної стрічки. Зараз ми пропонуємо більш функціональне та зручне вирішення проблеми.

**Отже, необхідно мати:**

- локальну мережу розбудовану за описом, що наведений в ч. 1. даної інструкції. (один ADSL-модем в режимі роутера та локальну мережу шкільних ПК);

- один, хай навіть морально застарілий, малопотужний комп'ютер з двома мережними картами. Друга мережна карта може бути придбана окремо (вона достатньо дешева) і самостійно встановлена в ПК в вільний слот PCI;

- дистрибутив ОС Linux. Ми використали спеціалізований дистрибутив **Ipfire 2.9** (http://www.ipfire.org ). Дистрибутив безкоштовний. Завантажити образ CD можна за посиланням
- http://downloads.ipfire.org/releases/ipfire-2.x/2.9-core49/ipfire-2.9.i586-full-core49.iso з сайта проекта, або за посиланням ftp://ftp.pmg17.vn.ua/pub/SchoolNet/ipfire-2.9.i586-full-core49.iso з ftp-сервера лабораторії інформаційних та комунікаційних технологій ФМГ№17 м. Вінниці. До речі, в папці SchoolNet лежать і PDF – версії всіх 3-х частин даної інструкції.

**Потрібно створити:**

- маршрутизатор (роутер), який би забезпечував вихід всіх ПК мережі в Інтернет з можливістю «справедливого» розподілу пропускної здатності каналу, гнучкої фільтрації небажаних Інтернет-ресурсів та простим управлінням через веб-інтерфейс.

# 2. Налаштування сервера

## 2.1 Інсталяція IPFIRE

### 2.1.1 Апаратні вимоги

Процесор: CPU Pentium (i586) з тактовою частотою на менше 333 МГц
Оперативна пам'ять: 512 Мб
Оптичний привід для читання CD- дисків : (потрібен лише на етапі інсталяції, може бути тимчасово встановлений).
Жорсткий диск: (IDE, SATA, SCSI), мінімальний розмір має становити 8 Гб
Мережа: 2 карти зі швидкістю передачі 10/100 Мбіт/с

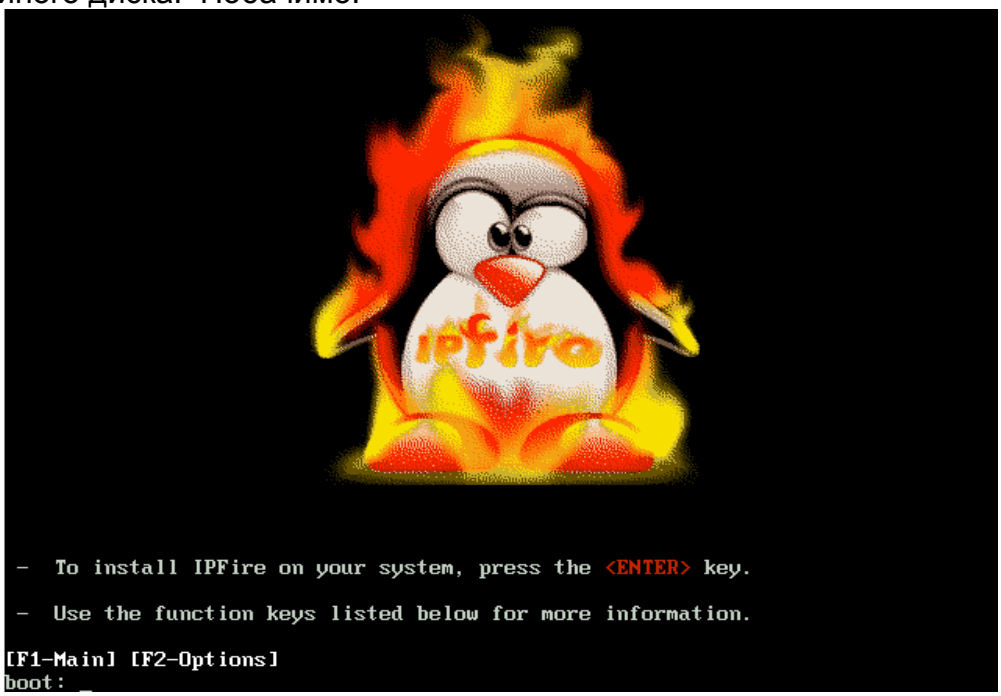
В нашому випадку було використано ПК з процесором Celeron 733 Мгц, ОЗУ 512 Мб, HDD 10 Гб. Такі ПК поставлялися в навчальні заклади в 1999-2001 рр. і в більшості випадках вже не використовуються в навчальному процесі.

### 2.1.2 Підготовка інсталяційного диска

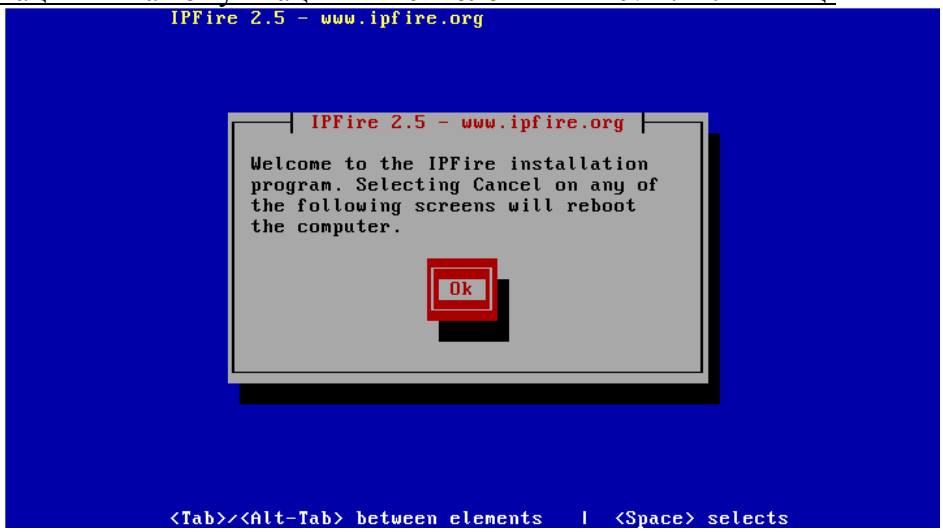
Завантажимо дистрибутив. Використовуючи будь-яку програму, що «вміє» це робити, наприклад Nero, розгорнемо образ на CD –диск.

### 2.1.3 Встановлення IPFIRE

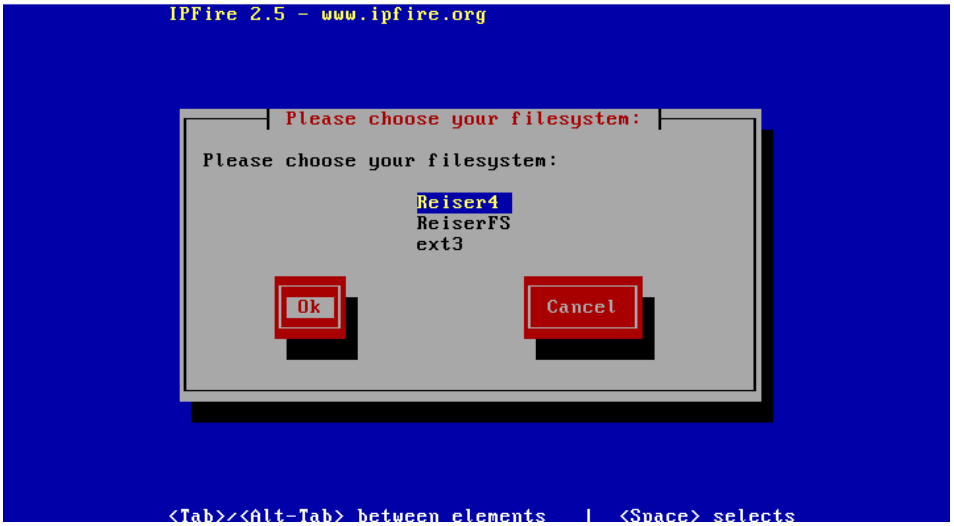
Заходимо в BIOS ПК та встановлюємо завантаження з CD. Вантажимося з нашого інсталяційного диска. Побачимо:



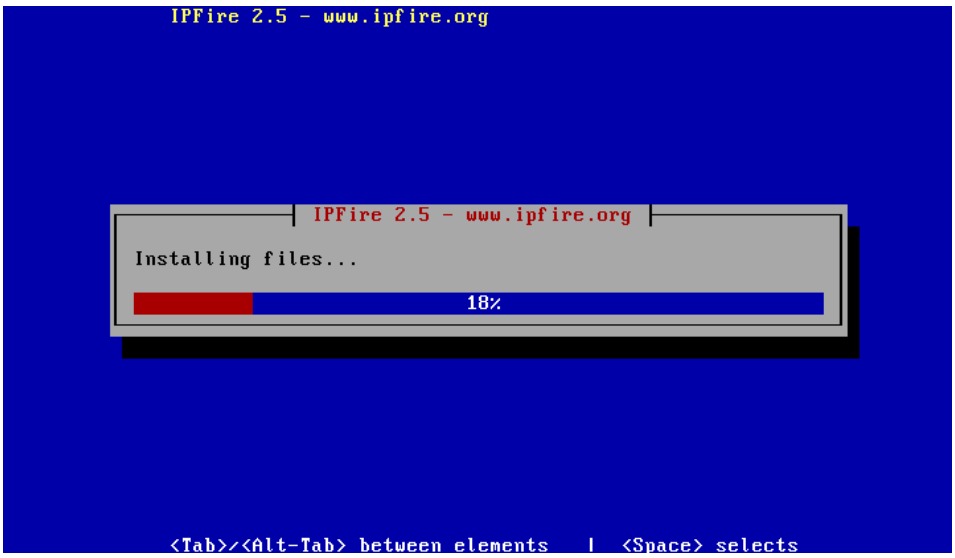

У випадку якщо монітор не підтримує розширення 1024 на 768 потрібно ввести з клавіатури команду ***novga*** і натиснути Enter, що призведе до зміни розширення монітору 640 x 480.
Через декілька секунд на екрані монітора з'явиться діалогове вікно, в якому буде запропоновано вибрати мову встановлення IPFIRE і веб-інтерфесу. Для вибору мови використовуються клавіші ↑ ↓ . Клавіші <Tab> та <Alt-Tab> дозволяють переміщуватись між елементами, клавіша <Space>(пропуск) дозволяє зробити вибір. Обираємо англійську (на жаль, української чи російської вам не запропонують).




Ви отримаєте попередження, що всі дані на вашому жорсткому диску буде знищено. На наступному кроці буде запропоновано вибрати файлову систему.



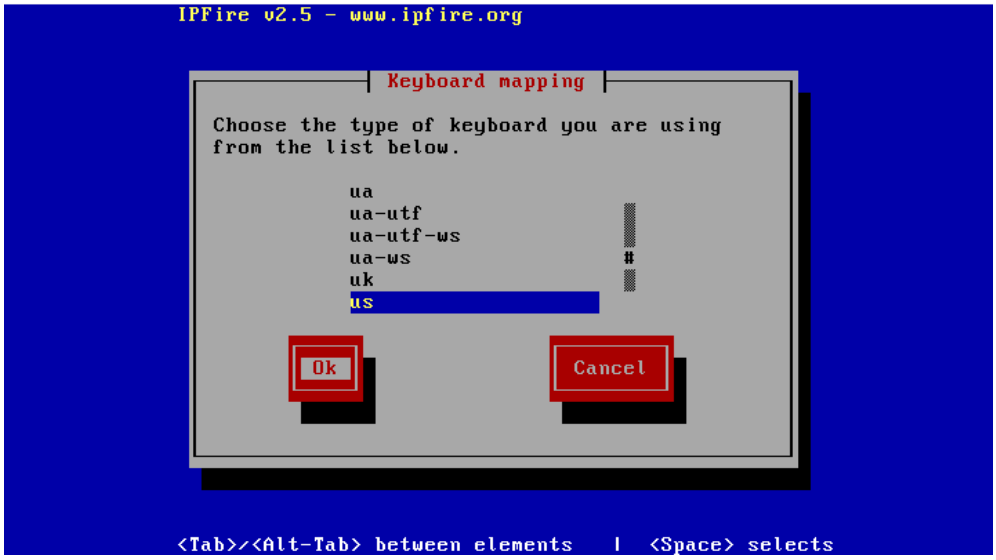

(в нашому випадку значення не має, обираємо будь-яку). Далі розпочнеться копіювання файлів

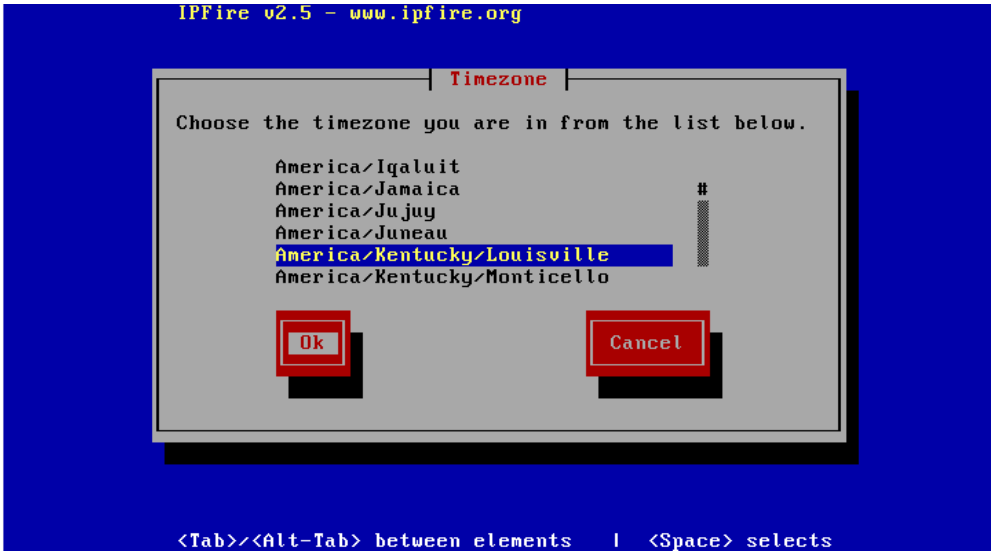


На завершення побачимо

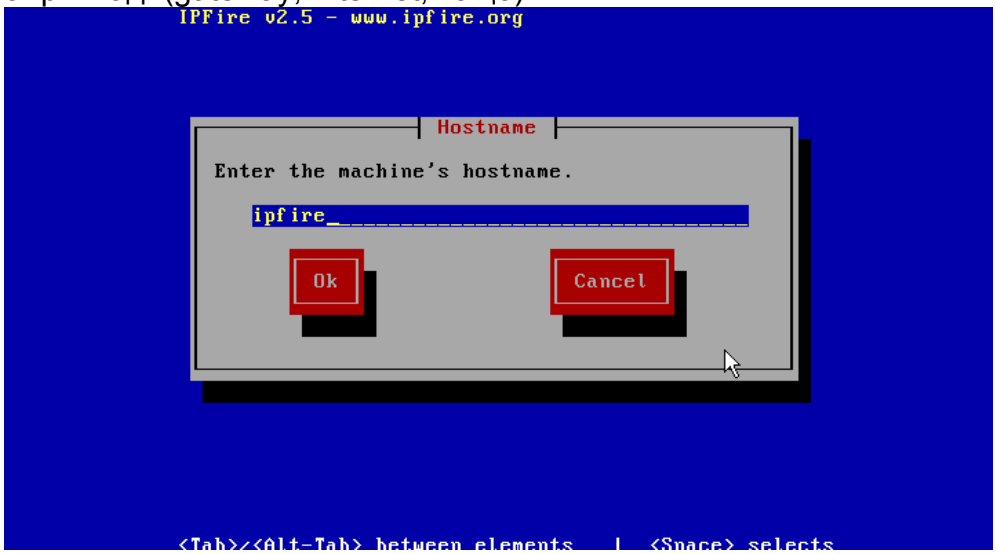

Виймаємо диск, як нам радить підказка, натискаємо Ок.

На наступному кроці буде запропоновано вибрати розкладку клавіатури і часову зону.



Робимо потрібний вибір. Після того як розкладка клавіатури та часова зона будуть обрані, потрібно буде вказати ім'я хоста, тобто назву за котрою IPFIRE буде відомий у локальній мережі. Наприклад: (gateway, Internet, тощо).




Далі потрібно вказати доменне ім'я. Якщо ви не використовуєте в локальній мережі внутрішній DNS , це ім'я може бути будь-яким.


У **наступному вікні потрібно задати пароль на вхід до системи**.

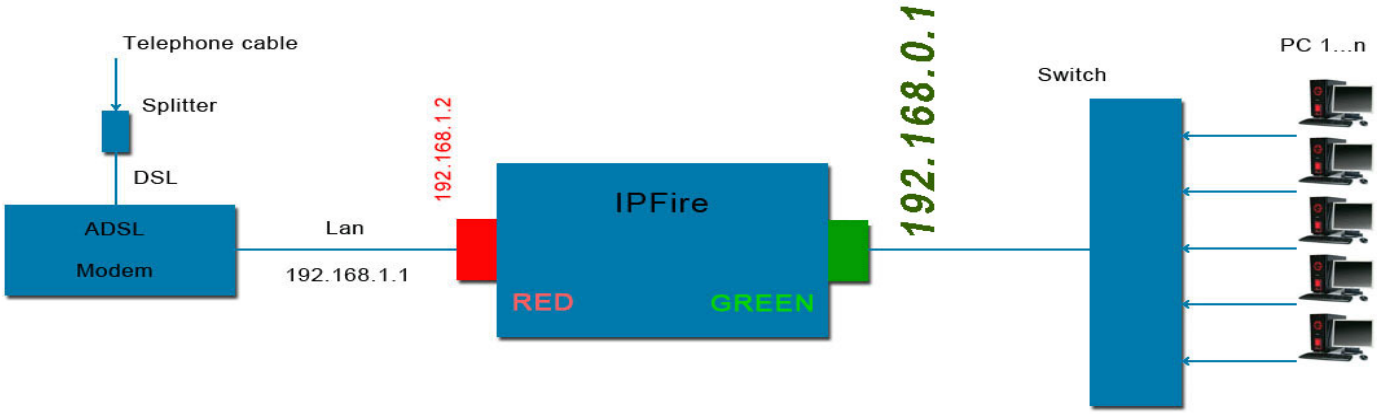
### 2.1.4 Налаштування мережі

Для стандартного налаштування мережі IPFIRE в нашому випадку потрібно 2 мережевих інтерфейси, - **RED** (інтерфейс, що «дивиться у світ»), та **GREEN** (інтерфейс, що дивиться у локальну мережу).

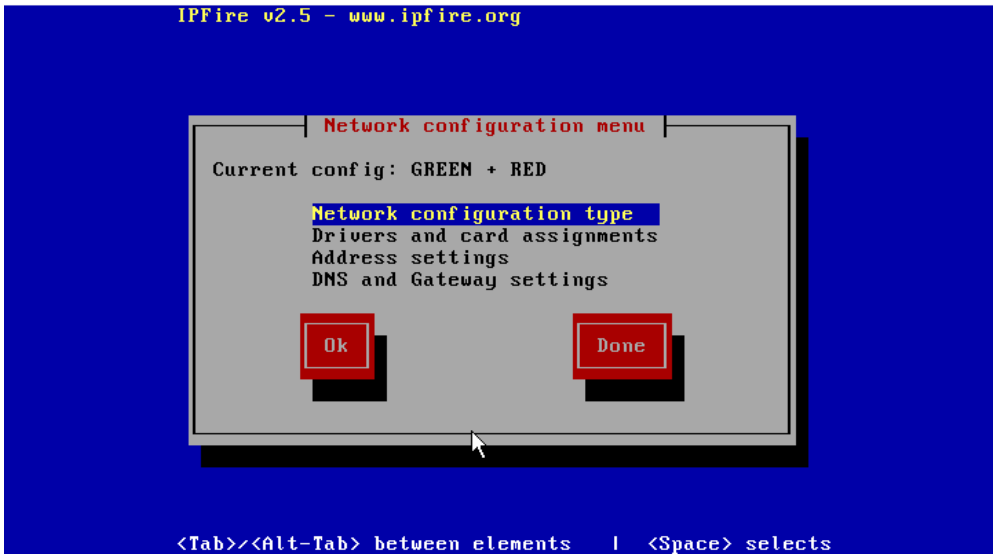
*Нагадаємо, що ми маємо налаштований модем-роутер, LAN – інтерфейс якого для нас буде «виходом в світ». В налаштування модема варто внести такі зміни (див.1 частину даної інструкції).* ***Це треба зробити до виконання наступних пунктів!***

*- забороняємо DHCP сервер. Він нам тепер не потрібен, адже в підмережі «модем-RED-інтерфейс» у нас буде лише 2 адреси. Хай, як і раніше, модем має 192.168.1.1, тоді RED-інтерфейсу ми присвоюємо в майбутньому 192.168.1.2.*

Для вирішення нашої задачі серверу IPFIRE потрібно 2 мережених інтерфейси: **RED** (інтерфейс, що дивиться у світ), та **GREEN** (інтерфейс, що дивиться у локальну мережу). Зрозуміло, що нова конфігурація мережі матиме такий вигляд:



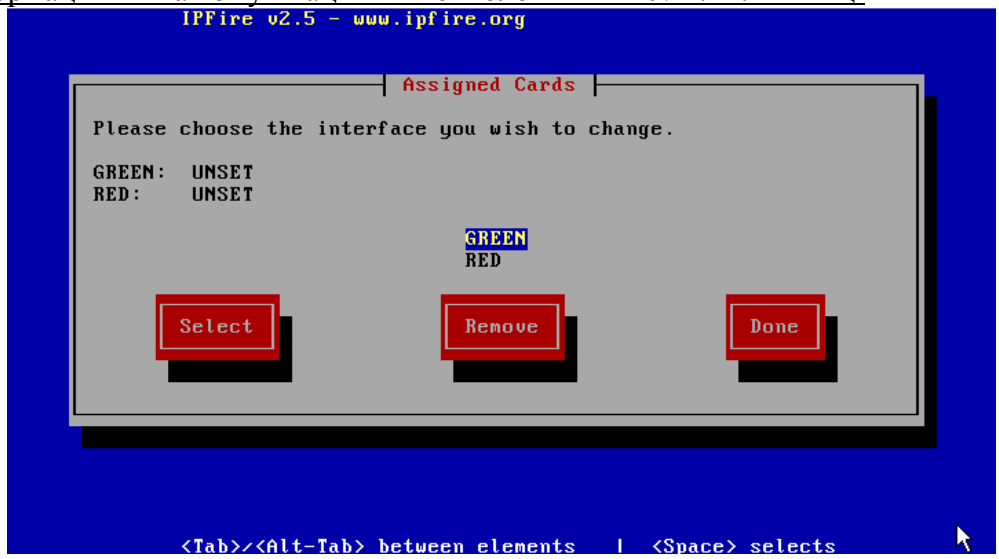

Повернемося до налаштування сервера. Наступне вікно діалогу буде таким:

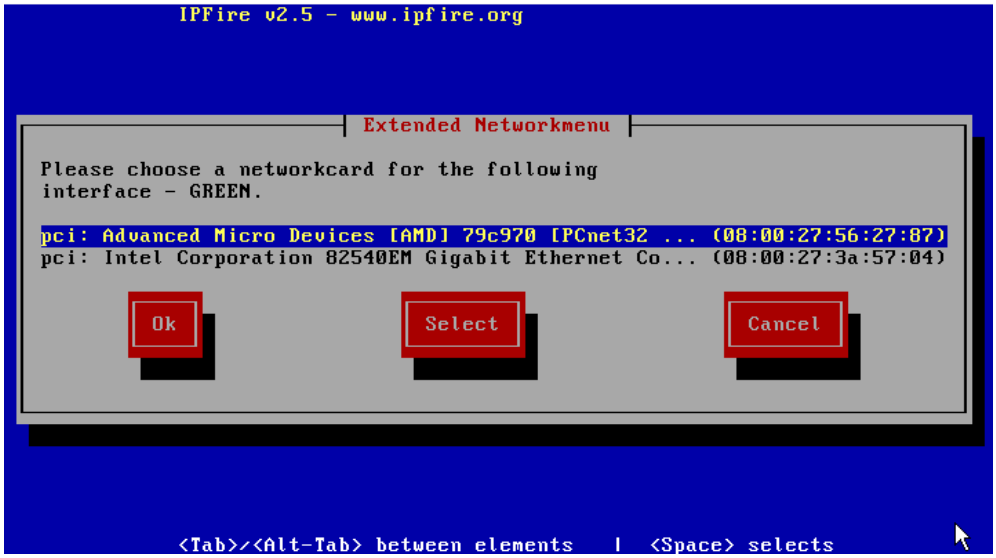



1. **Network configuration type** (зверніть увагу на напис Current config: Green + Red, що видно на попередньому малюнку, він повідомляє про те, що мережева конфігурація уже налаштована по замовчуванню на 2 інтерфейси). Система дозволяє використовувати до 4-х інтерфейсів, це можна зробити, обравши режим **Network configuration type , а далі один з режимів:**

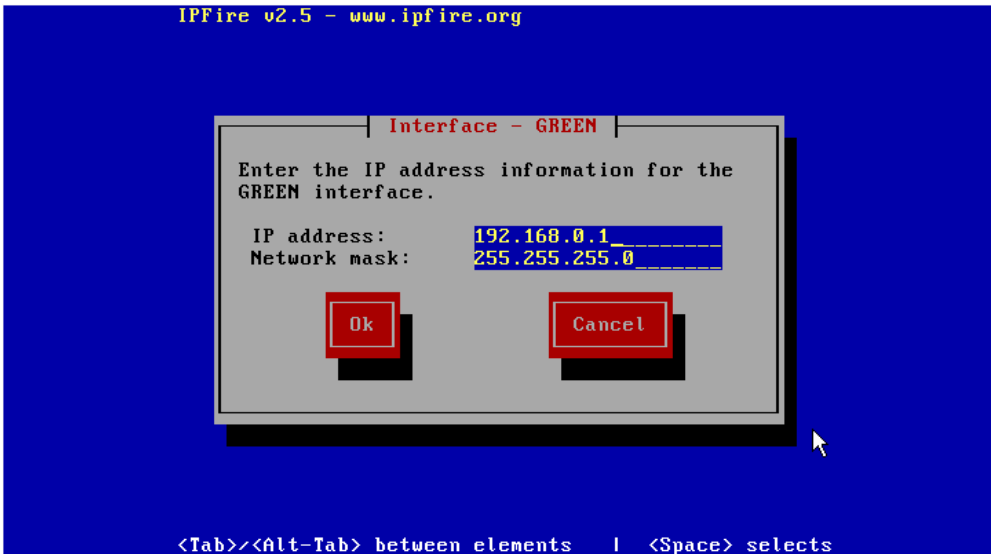
| | | |
|---|---|---|
| **Red** | WAN | зовнішня мережа, з'єднання з Internet |
| **Green** | LAN | внутрішня / приватна мережа, локальне з'єднання |
| **Orange** | DMZ | незахищена /серверна мережа, демілітаризована зона |
| **Blue** | WLAN | безпровідна мережа, окрема мережа для без провідних клієнтів |

Нам достатньо режиму з 2-ма інтерфейсами, адже у нас лише 2 мережних карти.
**Drivers and card assignments** надає можливість задати мережні інтерфейси.

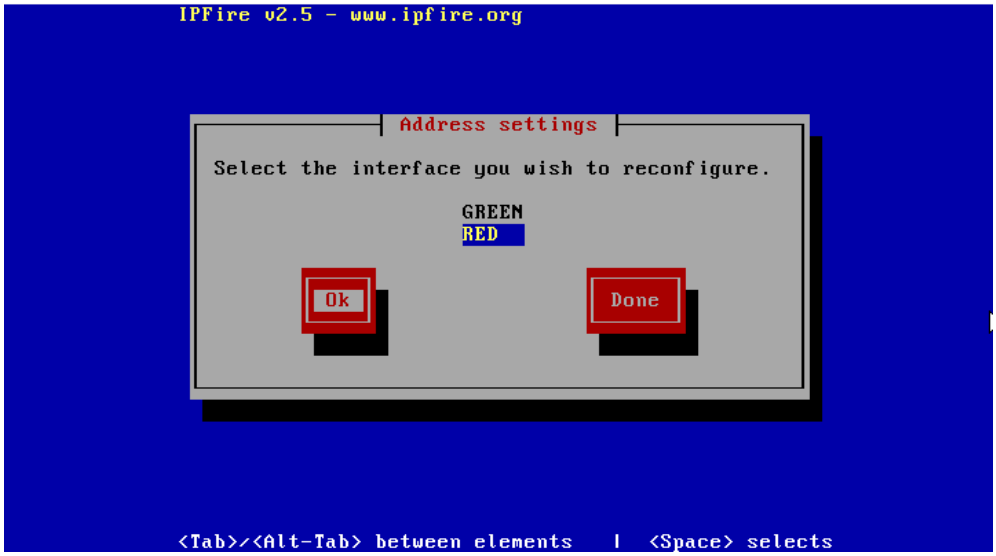


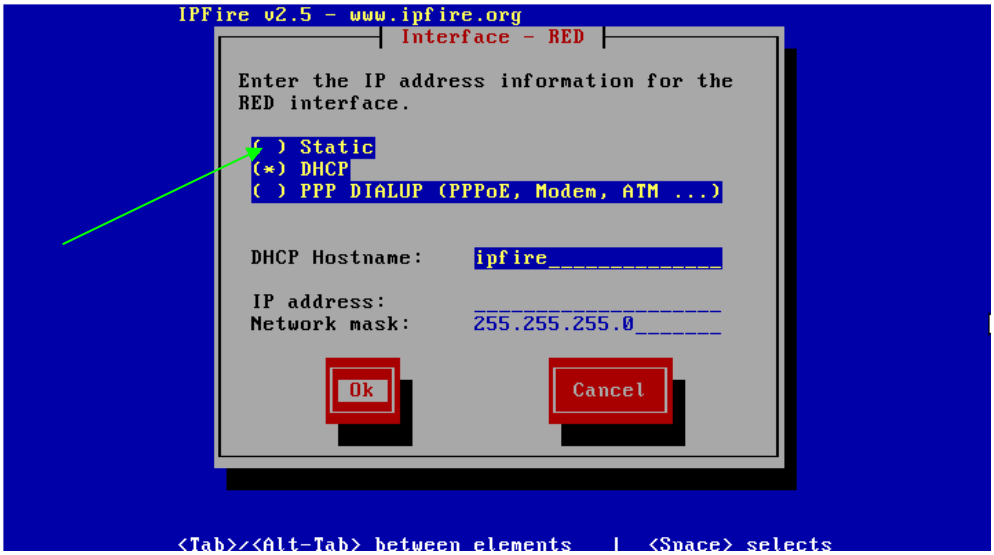




.**Address and settings** надає можливість присвоїти IP адреси мережевим інтерфейсам. В нашому випадку : **Red=192.168.1.2, Green=192.168.0.1 (мережна маска в обох випадках 255.255.255.0**



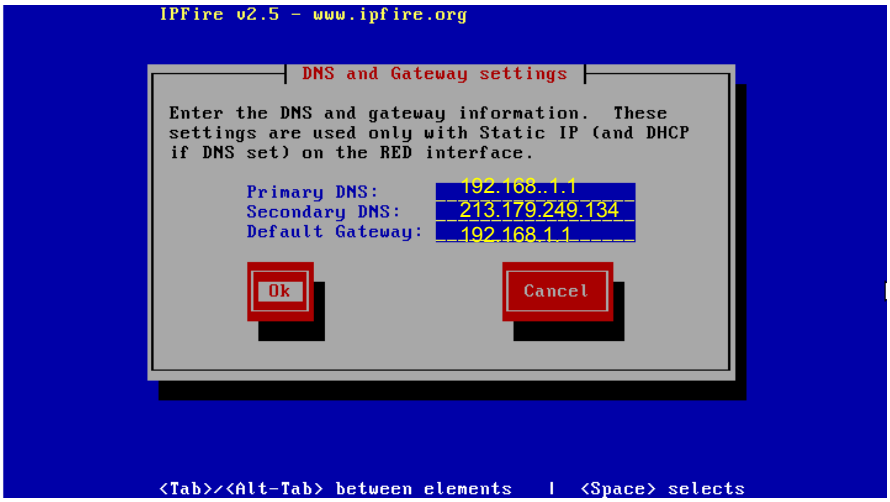

Налаштування зовнішнього (**Red**) інтерфейсу залежить від способу підключення до Інтернету




Для нашого випадку, коли **Red інтерфес підключено до LAN ADSL-**модема з адресою 192.168.1.1 ми в налаштуваннях інтерфейса обираємо Static і надаємо йому адресу 192.168.1.2 з маскою 255.250.250.0 **(на скріншоті не так!)**

**DNS and Gateway Installation** надає можливість налаштування DNS та Шлюза

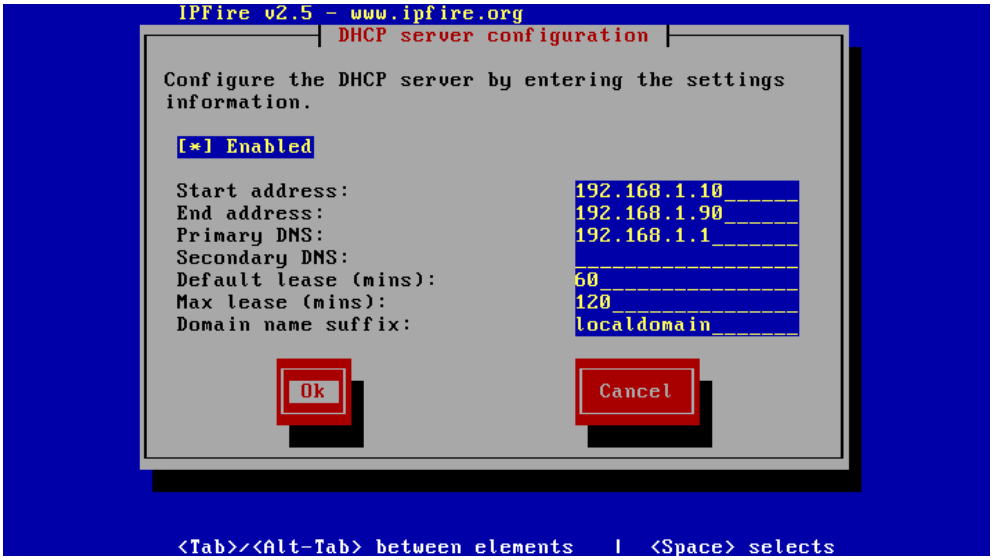


Тобто Primary DNS у нас буде модем, а Secondary – один з name-серверів Укртелекому. Власне, тут можна і не вписувати нічого, зокрема якщо ваш інтернет від іншого провайдера.

Налаштування **DHCP SERVER.** Для того, щоб ПК локальної мережі отримували всі налаштування автоматично, можливо облаштувати **DHCP SERVER**.

*Якщо ж з різних причин у вас на кожному ПК прописана статична адреса і інші налаштування (IP 192.168.1.XXX, Net Mask 255.255.0, DNS 192.168.1.1, Gatway 192.168.1.1) наступний крок пропускаємо.*

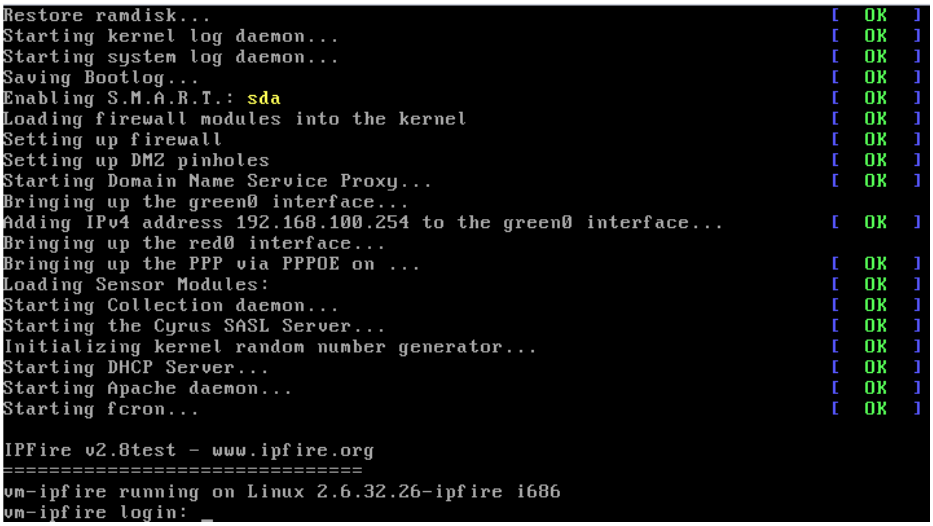
Для того щоб дозволити використання DHCP SERVER для **Green** інтерфейсу потрібно поставити галочку у параметрі **Enabled**, вказати початкову адресу, кінцеву адресу, основний DNS. За приклад можна взяти налаштування, що зображенні на малюнку.




***Примітка.*** *В подальшому ми будемо використовувати статичні IP-адреси клієнтів, так краще з багатьох міркувань, особливо коли кількість ПК в мережі не дуже велика. В такому випадку не слід ставити галочку* ***Enabled.***

Після чергового натискання на кнопку ОК потрібно перезавантажитися за допомогою команди reboot. Система перезавантажиться.


Обирайте перший (текстовий) режим. Хоча, якщо вам подобається графічний інтерфейс….

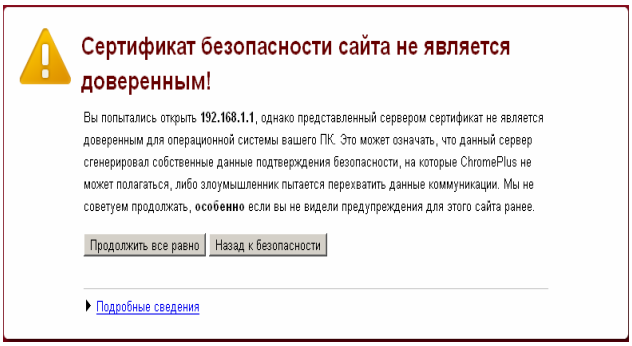



Ввійдіть в систему як користувач, використовуючи раніше введені логін та пароль. Якщо вам з якихось причин потрібно пройти процедуру налаштування повторно, виконайте команду **setup**.

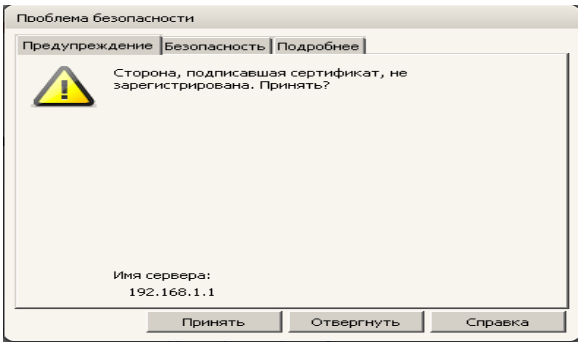
### 2.2.1 Використання веб-інтерфейсу.

Всі подальші операції можна (і потрібно) виконувати через веб-інтерфейс з будь-якого ПК локальної мережі. Тобто монітор та клавіатура (якщо ви все вірно налаштували на сервері) йому більше ні до чого ( від'єднуємо, сам системний блок ховаємо подалі, хай собі «жужить» тихенько. ;-)
Для доступу до налаштування через веб-інтерфейс у браузері потрібно перейти за посиланням https://ip_адреса_green_інтерфейсу:444
Наприклад: https://192.168.0.1:444
В залежності від браузера на екран буде виведено попередження:

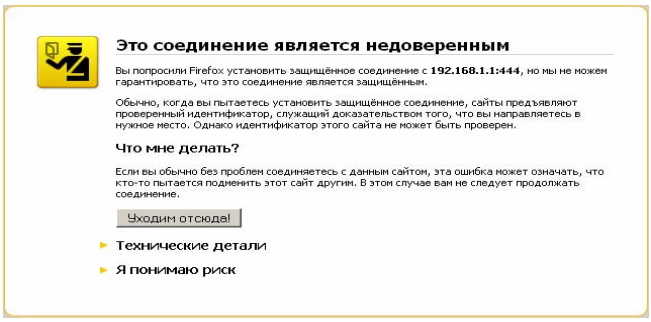
**Google Chrome**




**Opera**

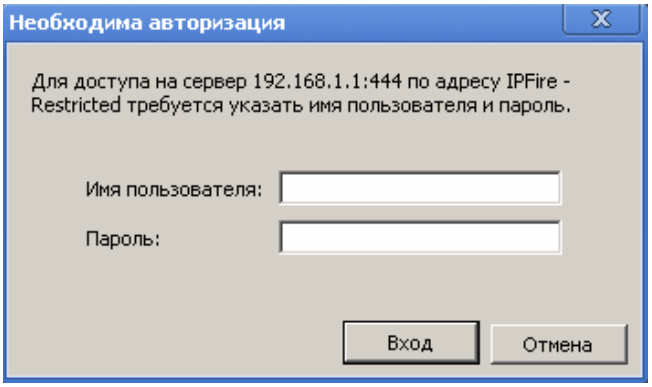



**Firefox**

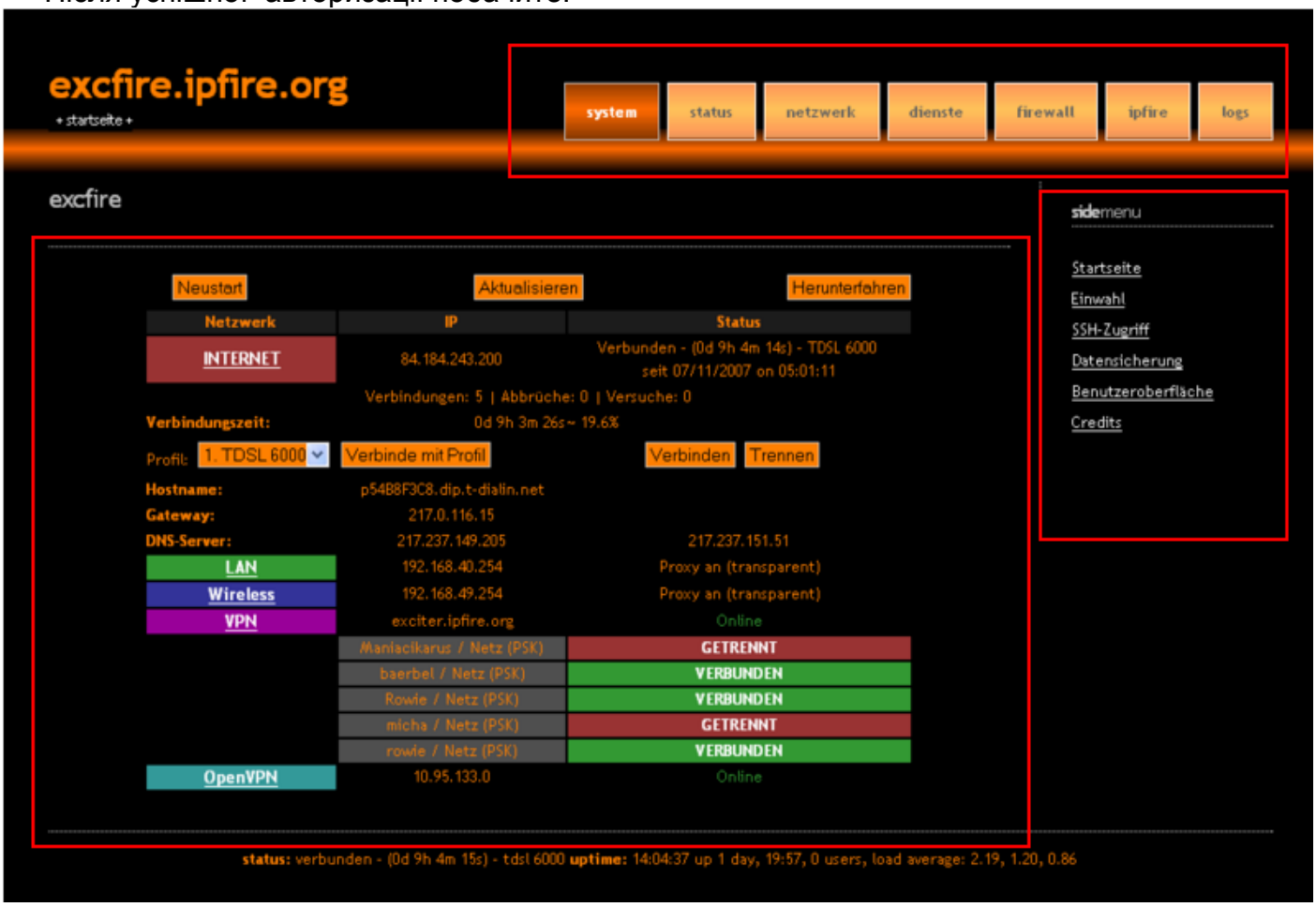



**Internet Explorer**

В будь якому випадку продовжуйте перегляд сторінки. Отримаєте форму авторизації. Вводите логін ( ім'я користувача) : **admin** пароль: ***той, що Ви встановлювали на вхід у систему.***

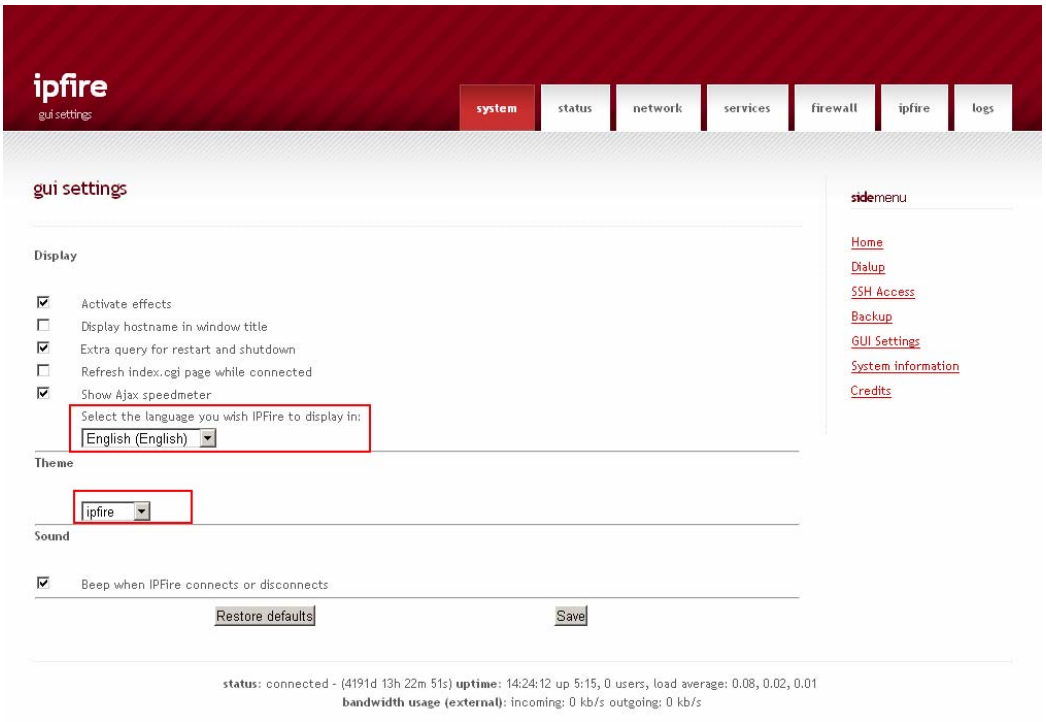



Після успішної авторизації побачите:




Веб-інтерфейс, що розділено на три частини, як видно на малюнку:
- у верхній частині знаходиться горизонтальне навігаційне меню;
- у правій частині знаходиться вертикальне навігаційне меню;
- у центрі знаходиться основний інформаційний блок.

Вигляд веб-інтерфейсу можна змінити на інший, перейшовши за посиланням **GUI Settings** у правій частині навігаційного меню (також можна змінити мову), вибравши потрібні налаштування у основному інформаційному блоці.

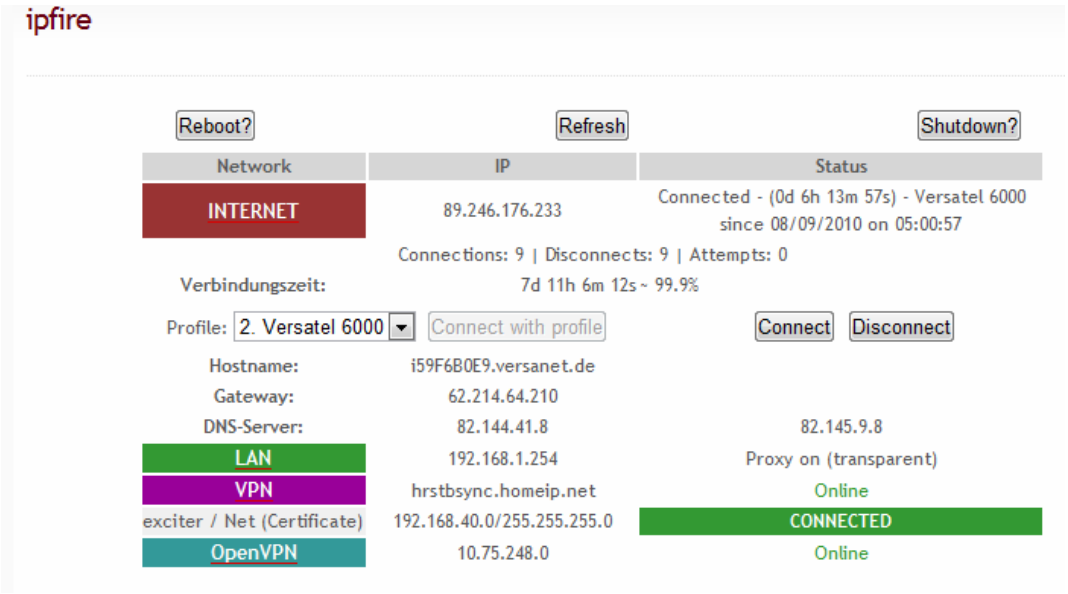



Після внесення змін потрібно натиснути на кнопку SAVE та перезавантажити сторінку клавішею F5, якщо все зроблене вірно, перед Вами з'явиться оновлений веб-інтерфейс, як показано на малюнку.

### 2.2.2 Вкладка "SYSTEM"

Вкладка SYSTEM горизонтального навігаційного меню надає доступ до налаштувань, перелік котрих відображається у вертикальному навігаційному меню, а саме:

**1.**Start page (початкова сторінка) Де відображаються мережеві інтерфейси, їхня IP адреса та стан активності.



Також у верхній горизонтальній площині знаходяться 3 кнопки за допомогою яких можна перезавантажити, оновити налаштування та вимкнути IPFIRE.

Reboot? (перезавантаження)

Refresh (оновлення налаштувань)

Shutdown? (вимкнення)

**2.**Dial-in (використовується тільки для модемного з'єднання) На даній сторінці ви можете налаштувати модемне з'єднання. В нашому випадку не потрібно нічого налаштовувати.

У розділі "PROFILE" можна вибрати тип підключення, непотрібне або помилкове підключення може бути видалене або відновлене.


Select (вибір)

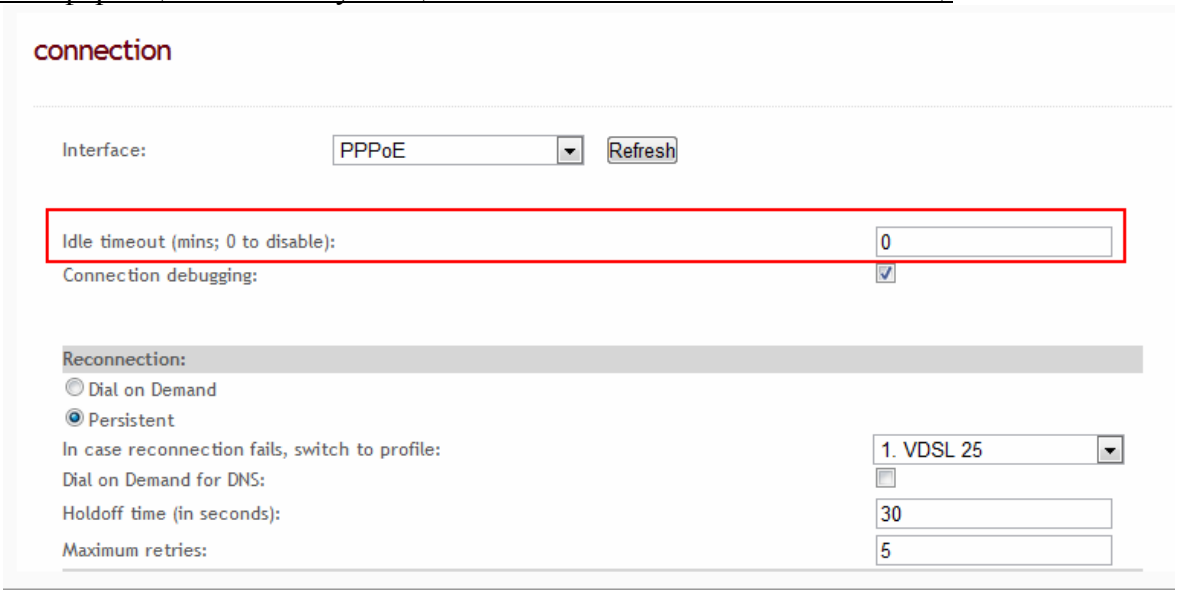
Delete (видалити)

Restore (відновлення)

***Подальші налаштування потрібні в випадку інших конфігурацій використання сервера, і в нашому випадку не потрібно нічого налаштовувати. Але можливо в майбутньому виникне потреба використовувати інше підключення, зокрема модем в режимі моста. Поки що текст дрібним шрифтом можна пропустити.***

Після того як Ви вибрали тип підключення, можете вибрати протокол з'єднання PPPoE або PPTP. (для ADSL модемів використовують протокол PPPoE)

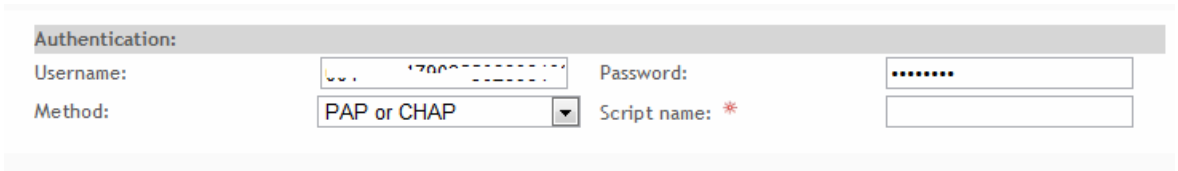

Для того щоб постійно перебувати у мережі internet значення idle timeout має бути 0.



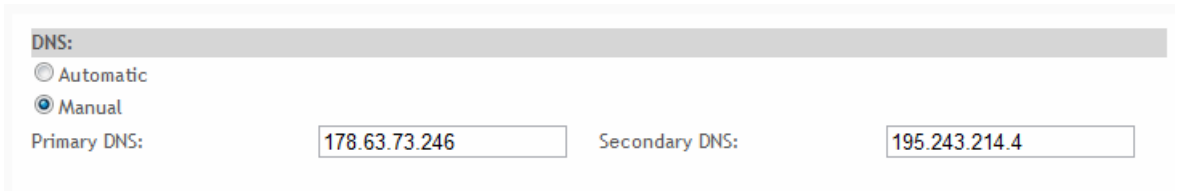

Додаткові параметри PPPoE можуть залишатись не змінними.

Розмір MTU **(**максимальний розмір блоку**)** потрібно виставити 1492.

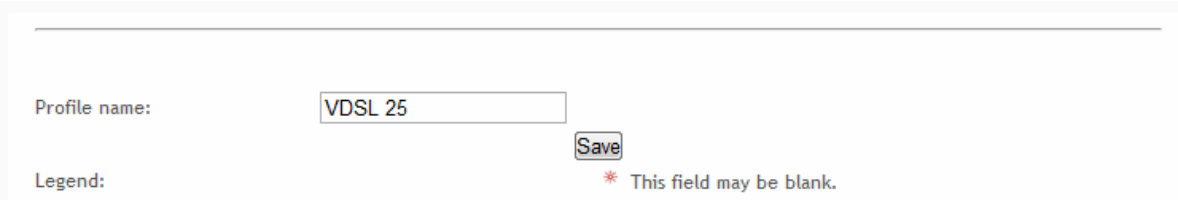

Наступний пункт пропонує Вам вказати логін та пароль, що були надані для доступу у internet, а також вказати тип передачі шифрування PAP чи CHAP краще вказати змішаний тип PAP or CHAP.




Налаштування DNS залежать від Вашого провайдера. В більшості випадків – Autovftic




Після усіх налаштувань Вам потрібно у “profile name” вказати тип підключення і натиснути кнопку “SAVE”.




**3.**SSH (***Secure SHell*** — безпечна оболонка)

Це не тільки програма, а й протокол для безпечного мереженого з’єднання з іншими віддаленими комп’ютерами.

По замовчуванню службу SSH відключено і її при необхідності потрібно увімкнути вручну.

У розділі Configure SSH Ви можете включи або відключити підтримку ssh.
Також у розділі доступно 3 режими:

start SSH permanently — постійний запуск служби;
start SSH temporarily for 15 minutes — тимчасовий на 15 хв;
start SSH temporarily for 30 minutes — тимчасовий на 30 хв.

IPFIRE використовує з причин безпеки 222 порт для SSH.

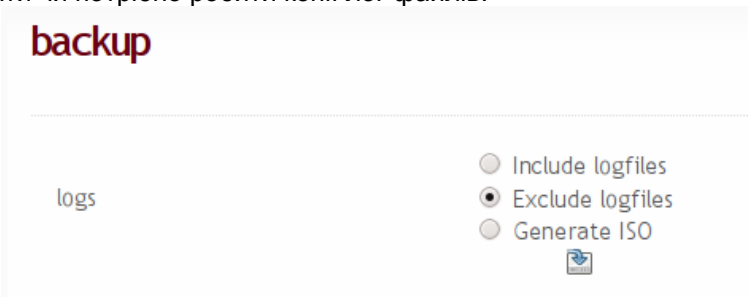
Якщо включений один з вище зазначених режимів Ви можете використовувати підключення до IPFIRE за допомогою SSH, використовуючи логін та пароль котрий був встановлений на вхід у систему.


Стандартний порт SSH прийнято вважати 22 (у IPFIRE порт 222) для того щоб у вас не виникло незручностей у роботі порт краще замінити на 22.

**4.**Backup (резервне копіювання)

Backup містить у собі конфігурацію та персональні налаштування IPFIRE.
Резервне копіювання можна робити як з врахуванням лог файлів так і без них. Якщо робити копію з врахуванням лог файлі то це буде займати багато часу.

Спочатку Вам потрібно вказати чи потрібно робити копії лог файлів.




Include logfiles включити підтримку резервного копіювання лог файлів;
Exclude logfiles відключити підтримку резервного копіювання лог файлів;
Generate ISO створити образ налаштунків та конфігураційних фай діл для запису на диску.

Для відновлення файлів з резервної копії у подальшому, важливо назву самої резервної копії не змінювати.

Для створення резервної копії Вам пропонується 2 варіанти:

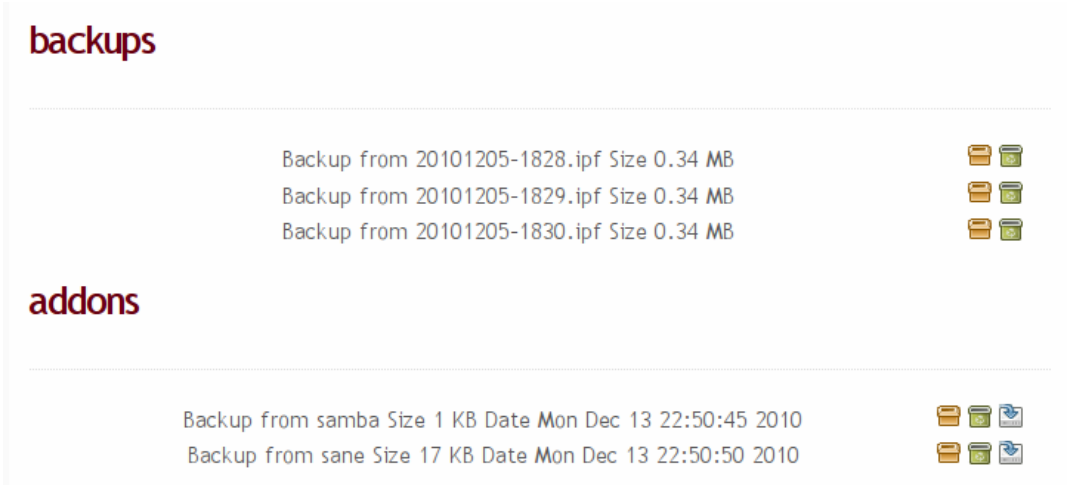
Створити копію конфігурації та персональних налаштувань;
Створити копію доповнень (програмні пакети).

- створення резервної копії

- завантаження резервної копії на персональний комп'ютер

- видалення резервної копії

- відновлення резервної копії



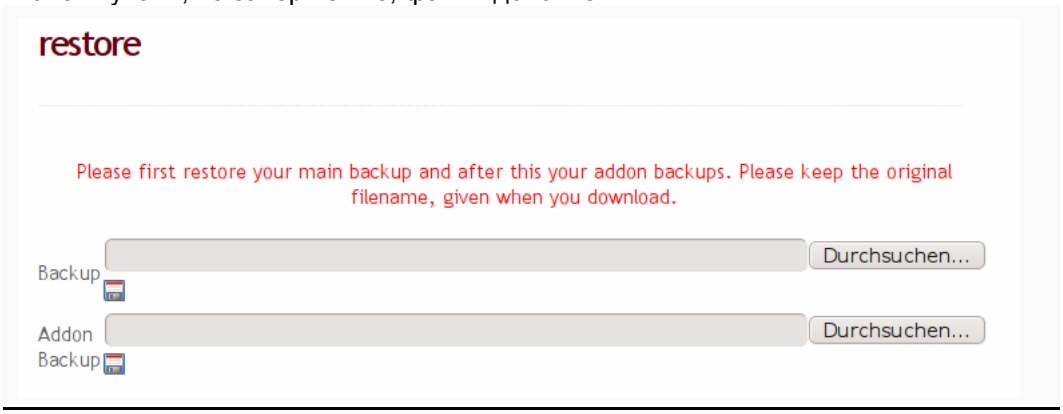

Резервне копіювання включає у себе наступні області:

- налаштування DHCP
- налаштування IPSec та OpenVPN
- налаштування DynDNS та firewall
- Port forwarding та зовнішній доступ
- Налаштування та правила Snort

Резервне копіювання доповнень, не дає можливості коректного відновлення, у випадку відновлення доведеться знову інсталювати доповнення і налаштовувати конфігурацію.

**Відновлення файлів.**

При відновленні файлів потрібно додержуватись певної послідовності, спочатку відновлювати файли конфігурацій та персональний налаштувань, по завершенню, файли доповнень.



# 3. Налаштування робочих станцій

## 3.1 Налаштування мережного з'єднання

Для організації доступу користувачів до мережі Інтернет необхідно виконати певні налаштування.

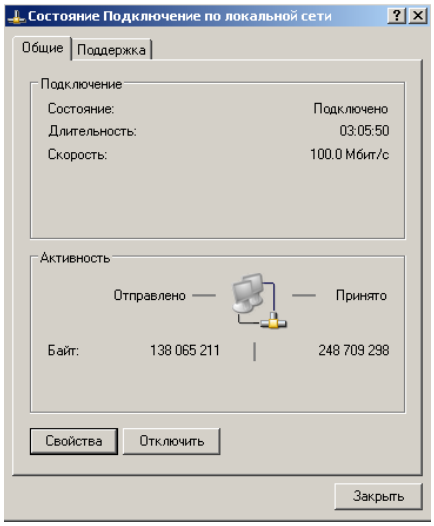
Нагадаємо топологію нашої мережі: ADSL-модем в режимі роутера з Lan-інтерфейсом 192.168.1.1, до якого підключено **Red** –інтерфейс сервера 192.168.1.2 (дивиться у Інтернет), а до Green-інтерфейсу (192.168.0.1, «дивиться» у локальну мережу) через некеровані свічі – всі комп'ютери закладу.

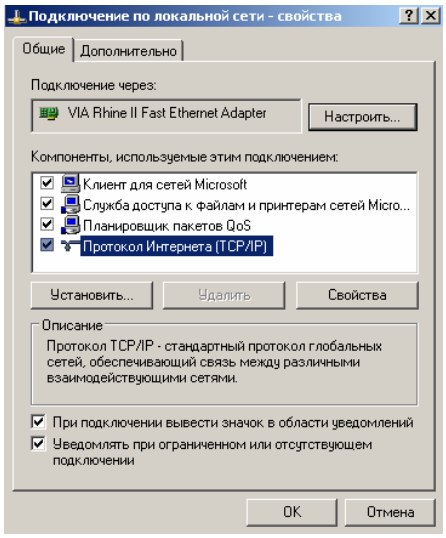
Спочатку потрібно змінити локальні мережені налаштування робочої станції користувача. (станція працює під однією з версій Windows). Перейдемо

***Пуск – Панель управления – Сетевые подключения***

Вибираємо потрібну мережену картку та клацнути двічі лівою кнопкою миші.

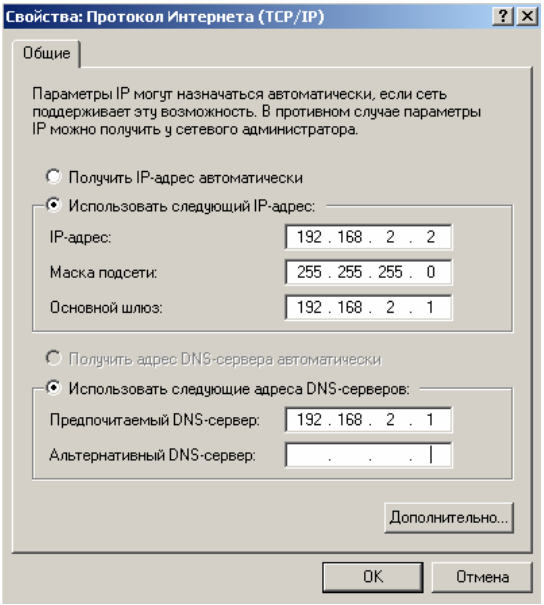
З'явиться вікно у котрому потрібно натиснути кнопку "Свойства"



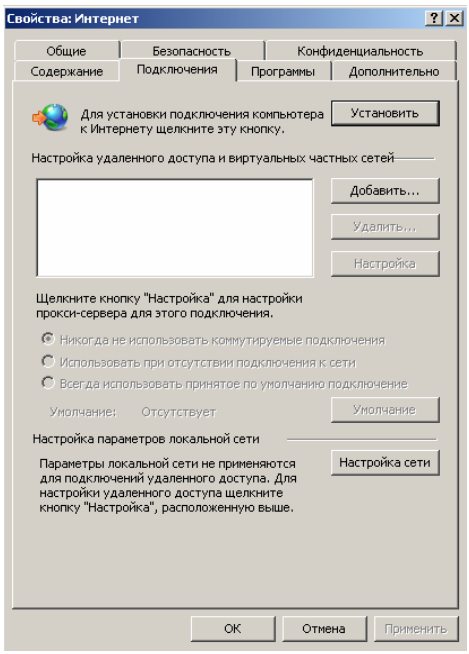

Далі потрібно вибрати **"Протокол Интернета (TCP/IP)"** та натиснути кнопку **"Свойства"** . У наступному вікні потрібно внести мережені налаштування, як вказана на малюнку та натиснути кнопку "ОК"

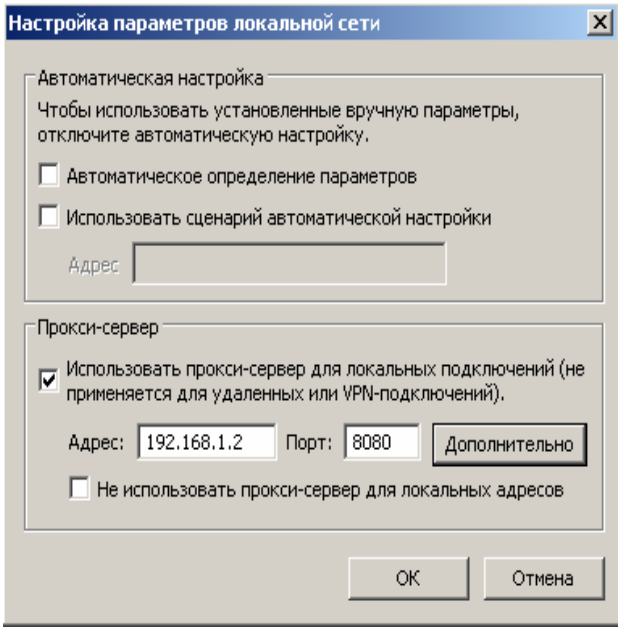
Таким чином потрібно налаштувати всі робочі станції, надаючи кожній з них унікальну IP – адресу 192.168.0.xxx. Ці налаштування слід зберегти, попіклувавшись про те, щоб користувач не міг їх змінити.



## 3.2 Налаштування браузера

Розглянемо послідовність дій в випадку використання браузера Internet Explorer. Перейдемо **Пуск – Панель управления – Свойства обозревателя**
Переходимо на вкладку **Подключения,** обираємо **Настройка сети**




відмічаємо **Использовать прокси-сервер для локального подключений,** в поле **Адрес** вводимо 192.168.0.1, в поле **Порт**: вводите 8080. Натискаємо **ОК**.
В інших браузерах налаштування проводиться аналогічно. Якщо на ПК використовуються кілька різних браузерів, налаштування слід робити в кожному. Варто потурбуватися, щоб непривілейований користувач не мав можливостей змінювати ці налаштування.

***Примітка.*** *Існують варіанти використання системи, що не потребують даних дій. Сервер можна налаштувати в режимі Transparent Proxy («прозорого» проксі), активізувати DHCP, а на клієнтських станціях в мережних налаштуваннях нічого не вказувати взагалі (ПК буде отримувати IP-адресу та адресу DNS автоматично). Але в цьому випадку різко зменшуються можливості адміністрування мережі, зокрема по встановленню обмежень доступу на небажані сайти. Тому ми рекомендуємо використовувати статичні IP-адреси та явну вказівку в браузері на використання проксі-сервера.*

# 4. Режими використання системи

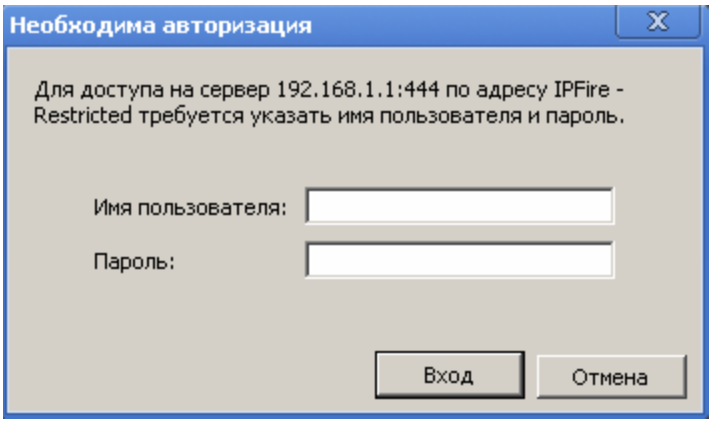
Система, з точки зору кінцевого користувача, може використовуватися в 2-х режимах – з авторизацією чи без, що надає додаткові зручності при використанні для різних потреб. Розглянемо ці режими та доцільність їх використання в різних ситуаціях

## 4.1 Режим роботи з авторизацією користувачів

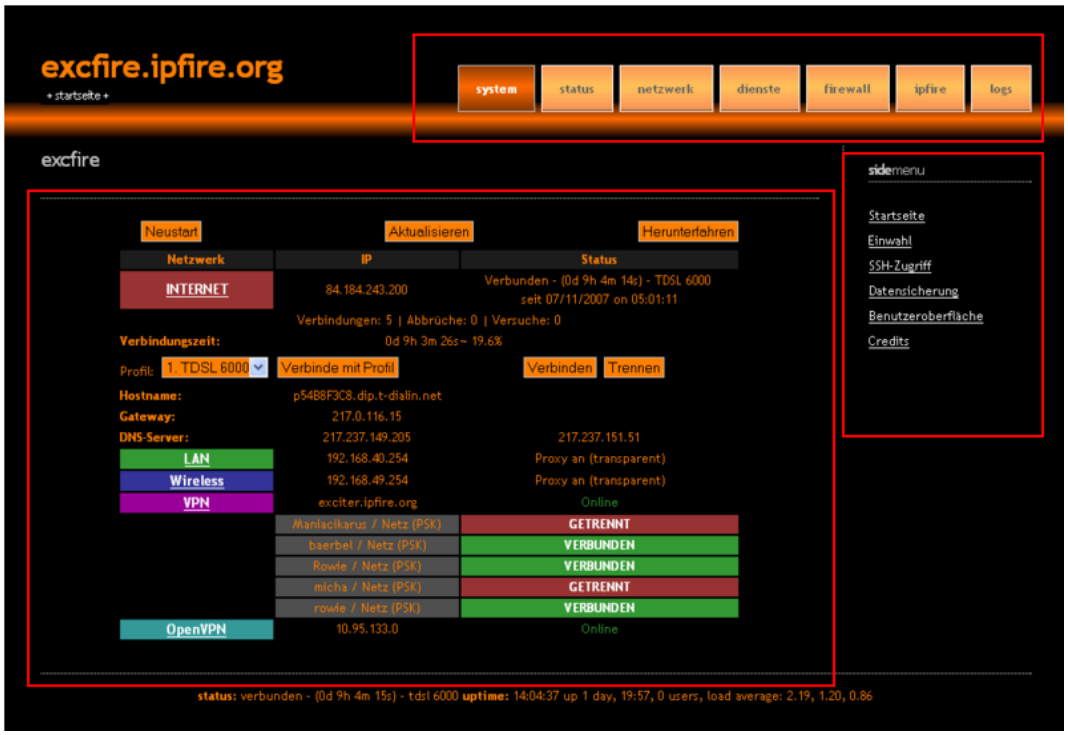
### 4.1.1 Налаштування сервера для роботи в режимі з авторизацією користувачів.

Підготуємося для використання такого режиму. Він є найбільш доцільним в більшості випадках використання Інтернету з навчальною метою, так як забезпечує гнучкі налаштування для кожної конкретної робочої станції

Наберемо в браузері https://192.168.0.1:444 та авторизуймося на сервері Логін (ім'я користувача): admin пароль: той, що Ви встановлювали на вхід у систему.



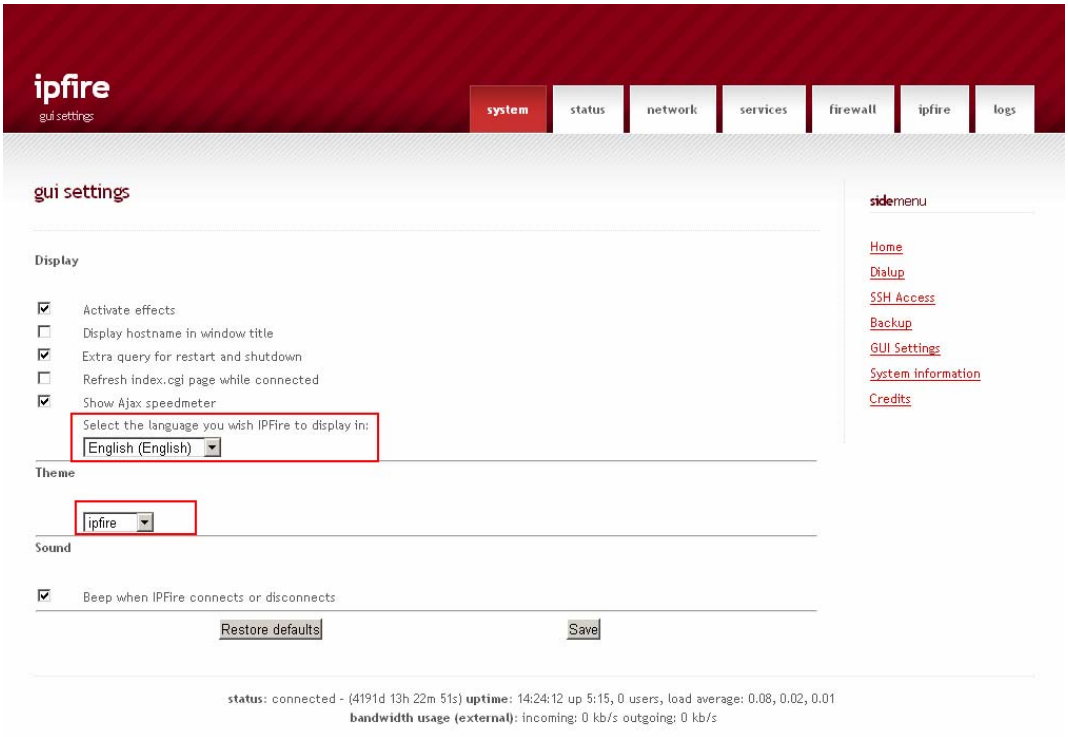

Після авторизації на екрані монітору з'явиться система управління IPFIRE через веб-інтерфейс.



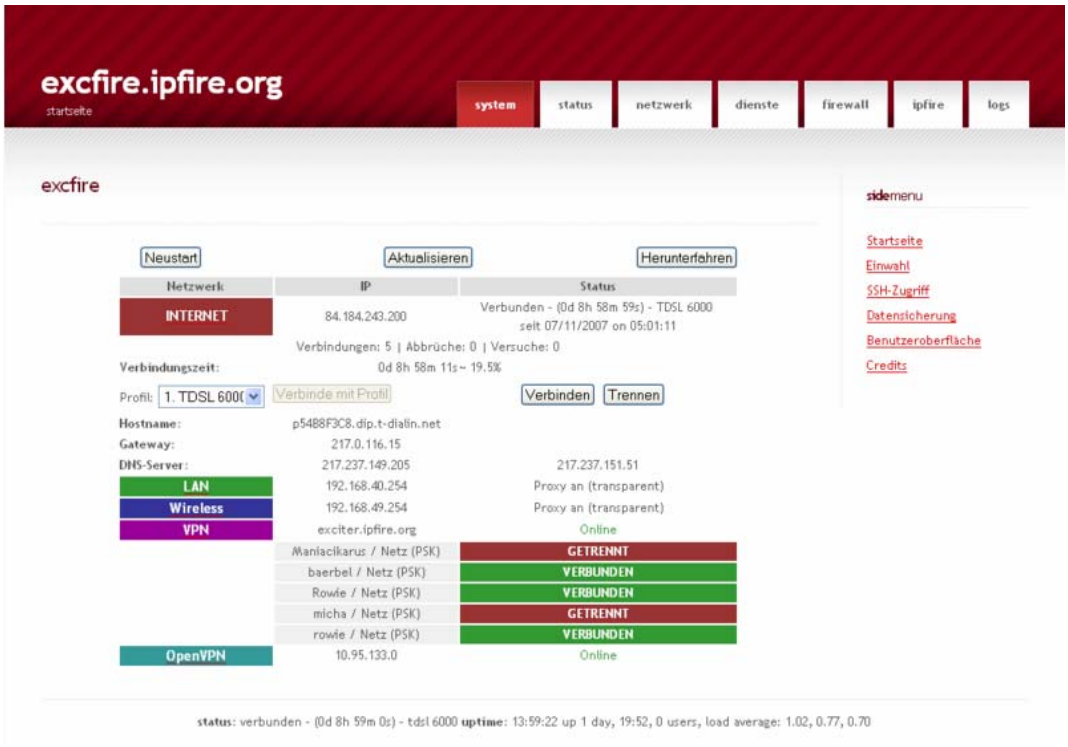

Веб-інтерфейс розділений на три частини, як видно на малюнку:

- у верхній частині знаходиться горизонтальне навігаційне меню;
- у правій частині знаходиться вертикальне навігаційне меню;
- у центрі знаходиться основний інформаційний блок.

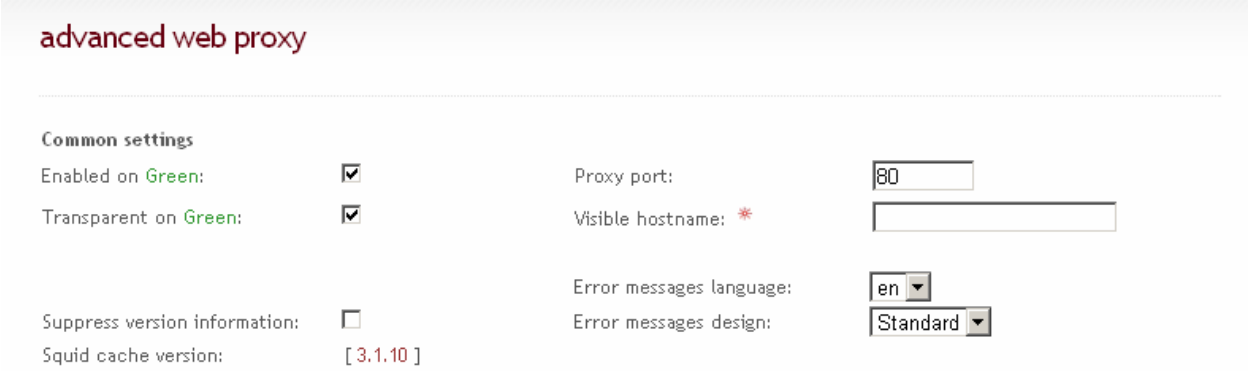
*Вигляд веб-інтерфейсу можна змінити на інший, перейшовши за посиланням **GUI Settings** у правій частині навігаційного меню (також можна змінити мову), вибравши потрібні налаштування у основному інформаційному блоці.*




*Після внесення змін потрібно натиснути на кнопку SAVE та перезавантажити сторінку клавішею F5, якщо все зроблене вірно, перед Вами з'явиться оновлений веб- інтерфейс, як показано на малюнку.*




Тепер Вам потрібно вибрати у горизонтальному меню вкладку “NETWORK” та вертикальному “ Webproxy ”

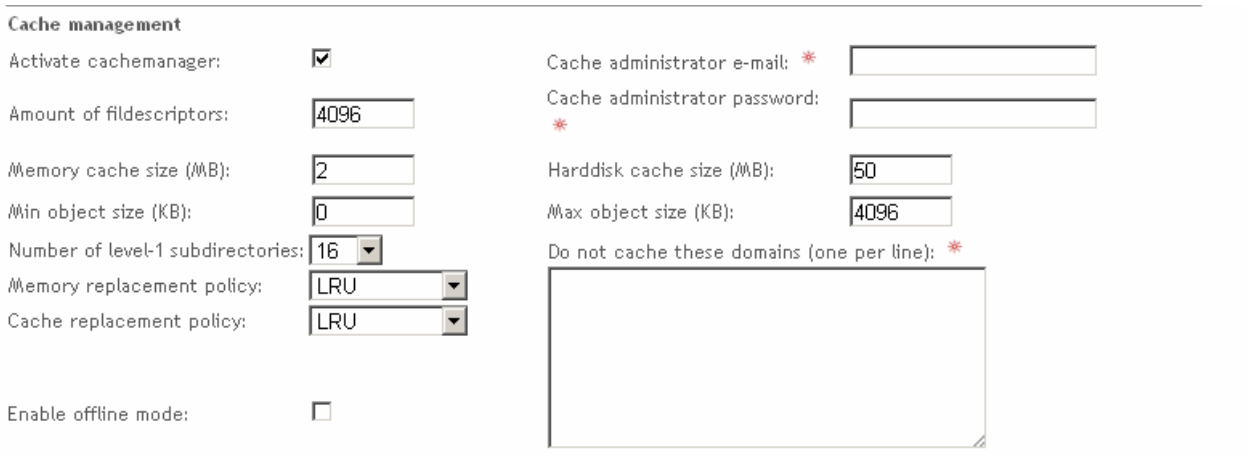



Потрібно зняти галочку з Transparent on Green та виставити Proxy port 8080. Після внесення змін перейдіть до завершення сторінки та натисніть кнопку SAVE – (зберегти). Це потрібно робити після внесення змін у кожному пункті.
Тим самим ми вказали, що на машинах користувачів «жорстко» прописаний проксі сервер

Пункт **Cache management (**налаштування параметрів кешування**).**

**Activate cachemanager -** активує кешування (встановити галочку)

**Memory cache size –** об’єм оперативної пам’яті котрий вказується для роботи з кешем (рекомендовано виставити 50 % від загальної кількості оперативної пам’яті) (виставте розмір пам’яті (наприклад: з 512 потрібно 256, з 256 потрібно 128).




**Harddisk cache size –** кількість вільного простору котре виділяється на жорсткому диску для роботи з кешем (рекомендований мінімум 1 Гб)

**Min object size –** мінімальний розмір кешованого об'єкту котрий не буде зберігатись на диск (можна залишити без змін)

**Max object size –** максимальний розмір кешованого об'єкту котрий не буде зберігатись на диск (можна залишити без змін)

**Number of level-1 subdirectories –** номер та рівень підкаталогів (рекомендовано виставляти **16)**

**Memory replacement policy –** дана опція визначає які об'єкти будуть видалені у разі закінчення вільно місця. (рекомендовано LRU)

**Cache replacement policy –** дана опція визначає які об'єкти будуть залишені у разі закінчення вільно місця а які ні. (рекомендовано LRU)

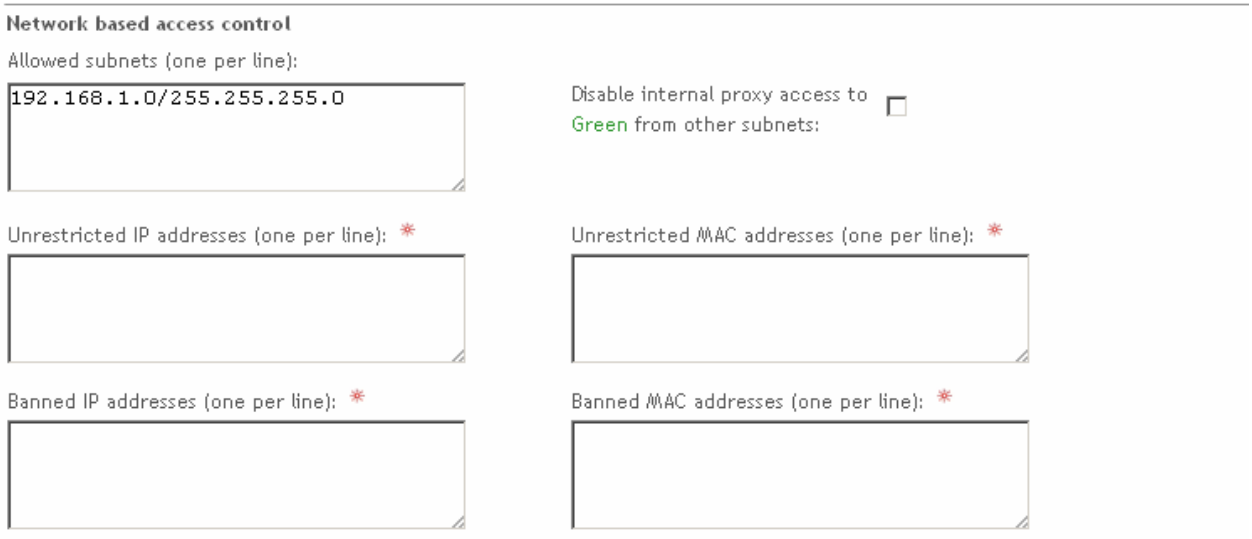
**Do not cache these destinations** – вказує список сайтів котрі не будуть кешуватись.

**Enable offline mode –** включення даної опції відключає перевірку кешування.(залишити без змін)

Після внесення змін перейдіть до завершення сторінки та натисніть кнопку SAVE – (зберегтись).

Пункт **Network based access control** (мережений контроль доступу на базі IP адреси)

обов'язково у **Allowed subnets – (**дозволяє доступ до мережі Інтернет тільки користувачам вказаної підмережі) вказати підмережу 192.168.0.0/24 або 192.168.0.0/255.255.255.0.




Після внесення змін перейдіть до завершення сторінки та натисніть кнопку SAVE – (зберегтись).

Пункт **Transfer limits**

Дозволяє задати обмеження на вивантаження та завантаження максимального пакету інформації у кілобайтах (KB).

*Доцільно використовувати для того щоб заборонити завантажувати з мережі Інтернет файли великих об'ємів (аудіо та відео контент, образи дисків тощо) не обмежуючи швидкість користувачам.*

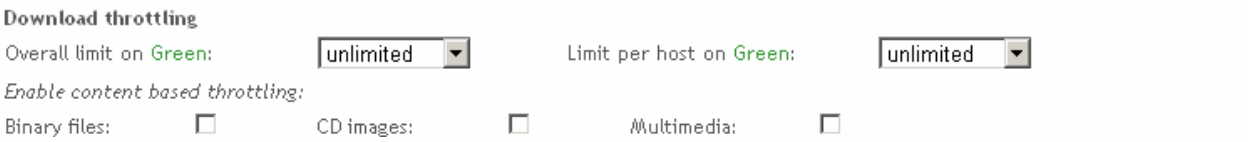
Max download size – максимальний файл котрий вигружається з Інтернет

Max upload size – максимальний файл котрий завантажується в Інтернет

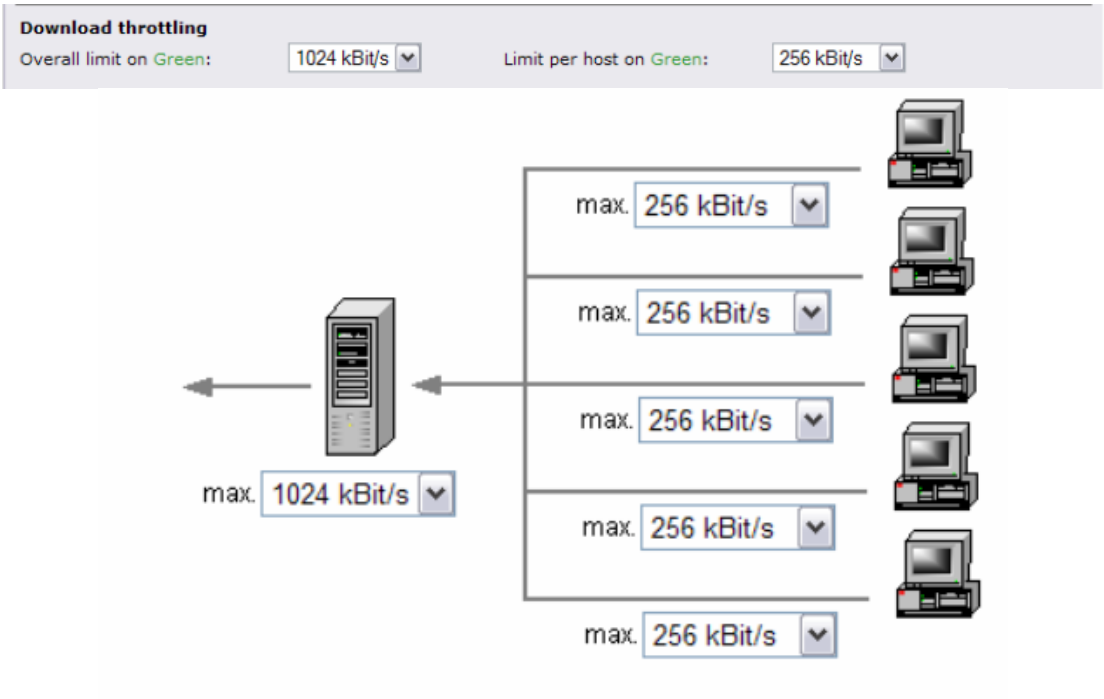

Після внесення змін перейдіть до завершення сторінки та натисніть кнопку SAVE – (зберегтись).

Пункт **Download throttling** (обмеження швидкості)

Дозволяє обмежити швидкість прийому на GREEN , а також з GREEN розподілити швидкість між користувачами.



Наприклад, якщо Ви виставите Overall limit on GREEN - (обмеження швидкості на GREEN) значене 1024 kBit/s, то на локальну мережу буде надходити 1024, а Limit per host on GREEN – (обмеження швидкості на користувачів) 256 kBit/s, відповідно користувачі отримають 256 kBit/s.




Після внесення змін перейдіть до завершення сторінки та натисніть кнопку SAVE – (зберегти).

Пункт **Web browser**

дозволяє ставити обмеження на використання певного програмного забезпечення для роботи у мережі Інтернет.

При неактивованому режимі має вигляд.


Для активації потрібно поставити галочку, перейти до завершення сторінки та натиснути кнопку SAVE – (зберегти).
У активованому.

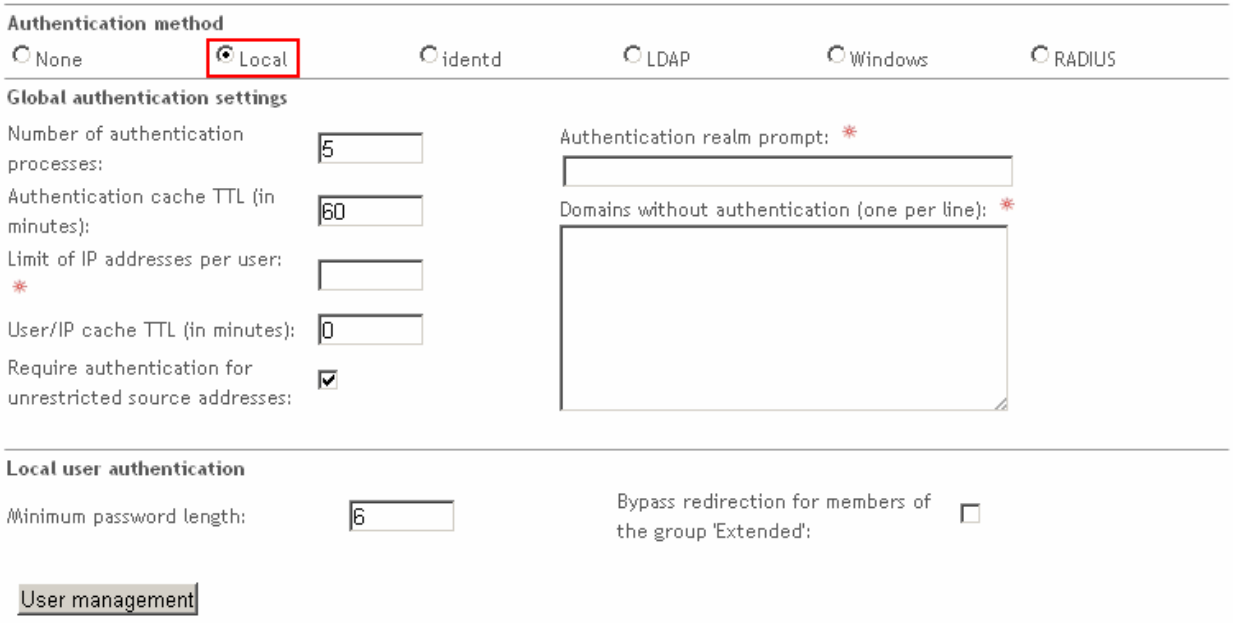

Після внесення змін перейдіть до завершення сторінки та натисніть кнопку SAVE – (зберегти).

Пункт **Authentication method** (метод авторизації)

дозволяє додавати користувачів для доступу до мережі Інтернет за логіном та паролем, або по дозволеній підмережі.

Вибираєте метод Local, переходите до завершення сторінки та натискаєте кнопку SAVE – (зберегти). Перед Вами з'явиться вікно з активованим методом Local.

Метод Local
Налаштування залишити по замовчуванню




Local має декілька пунктів налаштувань:

- Global authentication settings
- Local user authentication

## Global authentication settings

**Number of authentication processes**: - вказую число фонових процесів що очікують запит.

**Limit of IP addresses per user**: - обмеження IP адрес на одного користувача.

**Require authentication for unrestricted source addresses**: - вимагає авторизації у користувачів котрі не мають обмеження.

**Domains without authentication (one per line):** - сайти на котрі дозволяється доступ без авторизації.

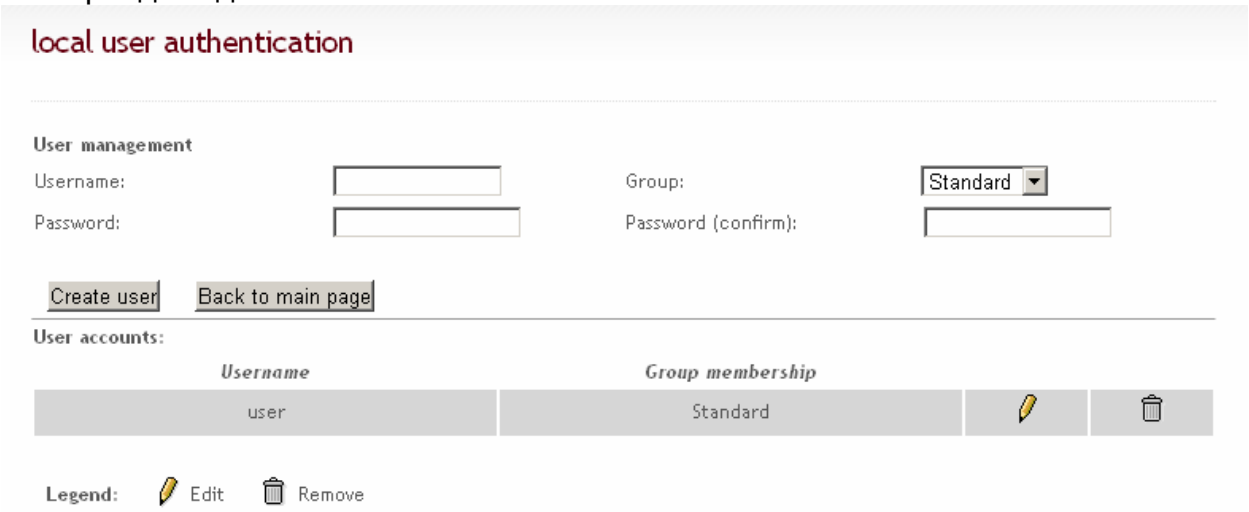
## Local user authentication

**Minimum password length**: - вказує довжину паролю користувача.

**Bypass redirection for members of the group 'Extended'**: - обхід налаштунків тільки для користувачів групи 'Extended'.

### 4.1.2. Створення користувачів

Для створення користувача потрібно натиснути кнопку “User management”
Ви перейдете до **local user authentication**




Пункт **User management**

**username** – ім’я користувача
**password** – пароль користувача
**group**
standard – група на котру діють вказані обмеження ,
extended – група на котру не діють вказані обмеження,
disables - група котра блокує користувача без втрати логіна та пароля групи
password (confirm) – підтвердження паролю

**Пункт User accounts**

username – ім’я користувача

group membership – членство у групі

- редагування запису

- видалення запису

Отже:
Для створення нового користувача потрібно натиснути кнопку **User management** котра Вас перемістить до **local user authentication**, далі заповнити поля розділу **User management**

Наприклад:

| | | | |
|---|---|---|---|
| username | User1 | group | standard |
| password | 123456 | password (confirm) | 123456 |

та натискуєте кнопку "**Create user**".

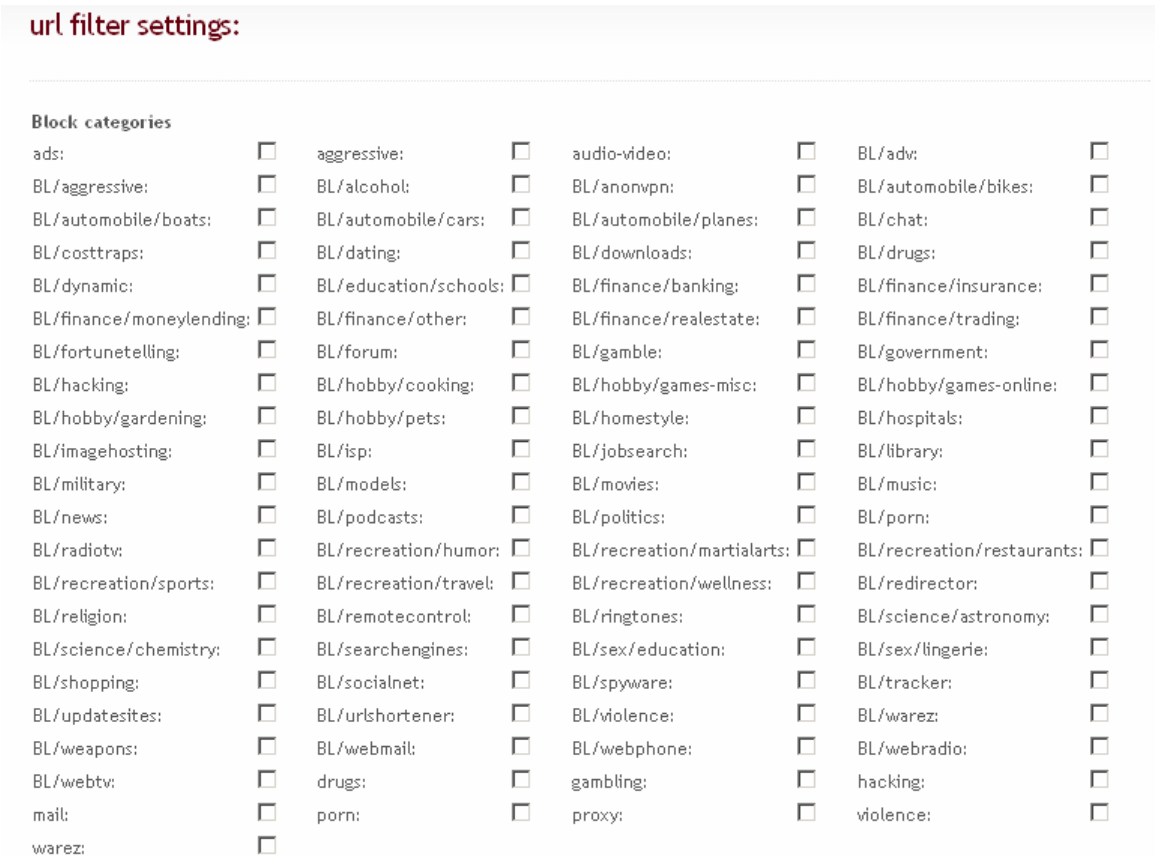
За допомогою кнопки "**back to main page** " повертаєтесь до головної сторінки де натискаєте кнопку SAVE AND RESTART – зберегтись та перезавантажити проксі-сервер.
***Примітка*** *В випадку комп'ютерного класу логічно завести користувачів за кількістю ПК, надавши їм логічні імена (напиклад,* ***User1, User2,…,User10****) та встановивши несекретні паролі (напиклад,* ***pasUser1, pasUser2, …,pasUser10****). Всіх цих користувачів сілід віднести до групи* ***standart.*** *На цю групу поширюються всі обмеження, що встановлено на сервері. Також варто створити користувачів, на яких обмеження не поширюються (boss,☺, sekretar, teacher…) та віднести їх до групи* ***extended.*** *Зрозуміло, що паролі таких користувачів повинні бути секретні для учнів.*

Даний режим буде основним для роботи з системою. Далі ми детально розглянемо механізми встановлення обмежень небажаногоо контента.

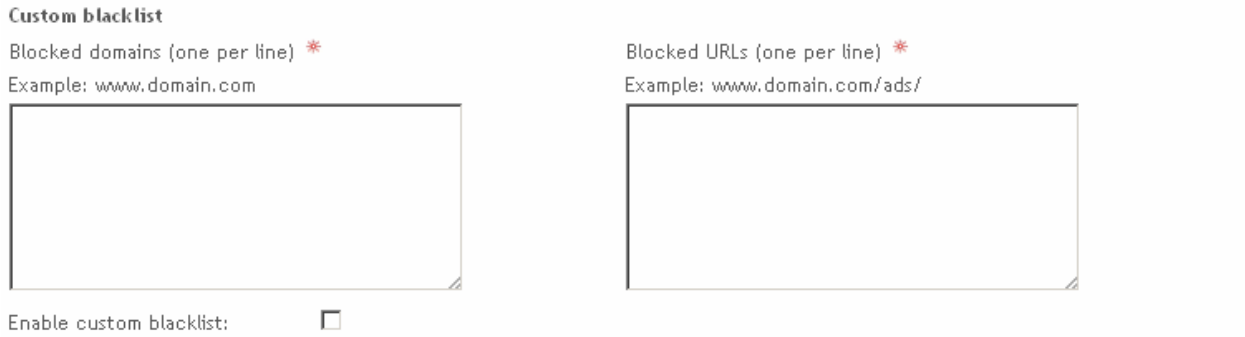
### 4.1.3. Організація фільтрації небажного та шкідливого контента

Зайдемо на сервер через веб-інтерфейс (див п.4.1.1) як адміністратор, в горизонтальному меню **Network,** далі **Content Filter.**
Отримуємо можливість блокувати небажаний контент.

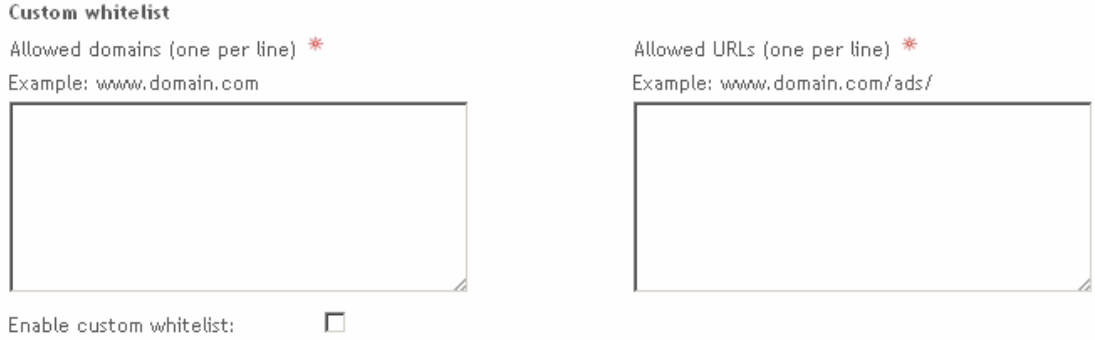
**url filter settings** - дозволяє вибрати категорію для блокування, але якщо фільтр має багато записів то швидкість передачі інформації на користувача зменшиться у рази. Краще використовувати блокування контента по певним словам.



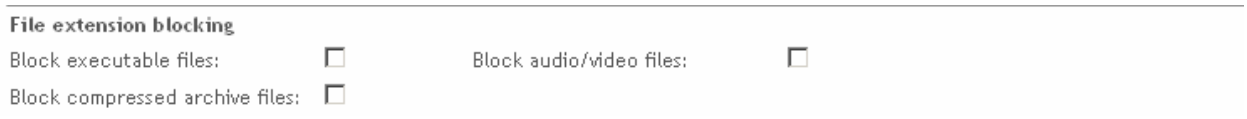

**Custom blacklist -** блокувати контент за доменом та URL адресою.
**Blocked domains** – блокування за доменом
**Blocked URL** – блокування за URL адресою
**Enable custom blacklist** – активує чорний список




**Custom whitelist -** дозволяє доступ тільки до вказаних сайтів за доменом та URL адресою.
**Enable custom whitelist** – активує білий список

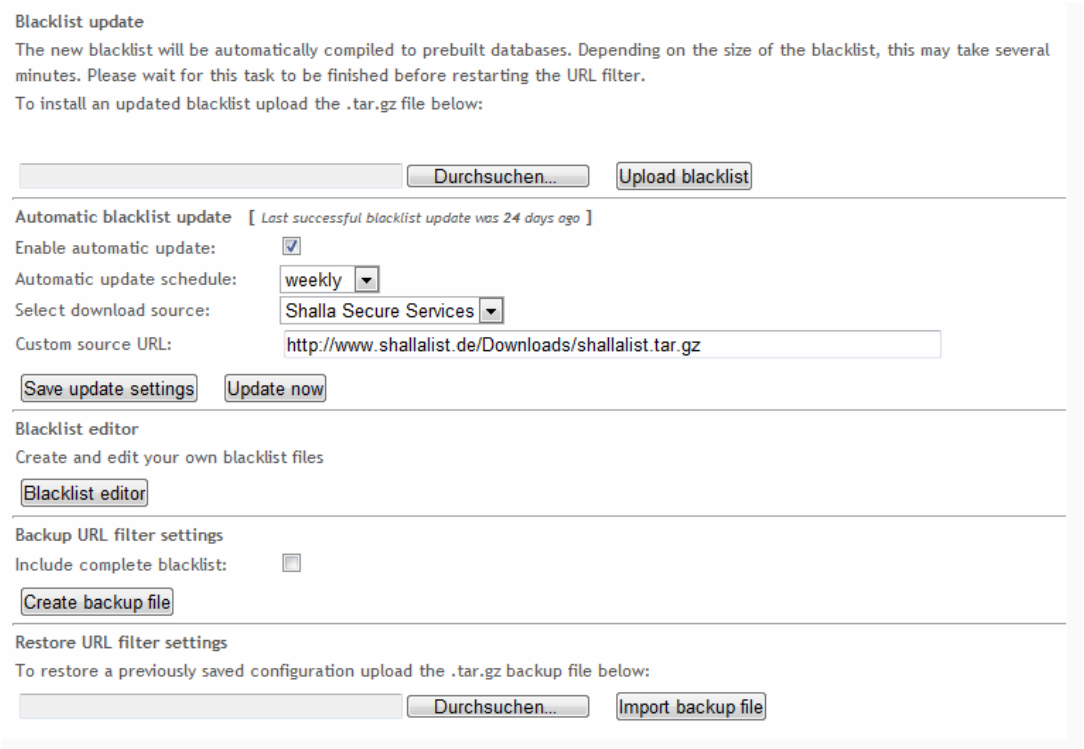


**File extension blocking** - дозволяє блокувати завантаження по типу файлу.




**Network based access control** - дозволяє обходити фільтрові обмеження вказаним адресам.
**Unfiltered IP addresses** – IP-адреси користувачів, яким дозволено обходити фільтр
**Banned IP addresses** – IP –адреси користувачів, які не обслуговуються


***Примітка**. Поряд з механізмом груп, дана можливість додає гнучкості в організації фільтрації доступу. Зокрема, можна на змінюючи групи користувача, надати чи позбавити йому обмеження.*
**Blacklist update** - дозволяє обновити базу «блеклистів» з вказаного джерела.




Для блокування за ключовими словами потрібно обрати у горизонтальному меню вкладку **NETWORK** та вертикальному **Content Filter** та прокрутити до **Custom expression list.**
У полі **Blocked expression** вписуємо слова, які є небажаними як і в запитах, так і в отриманому контенті.

**Приклад:**

насилля
вбивство
наркотики
……

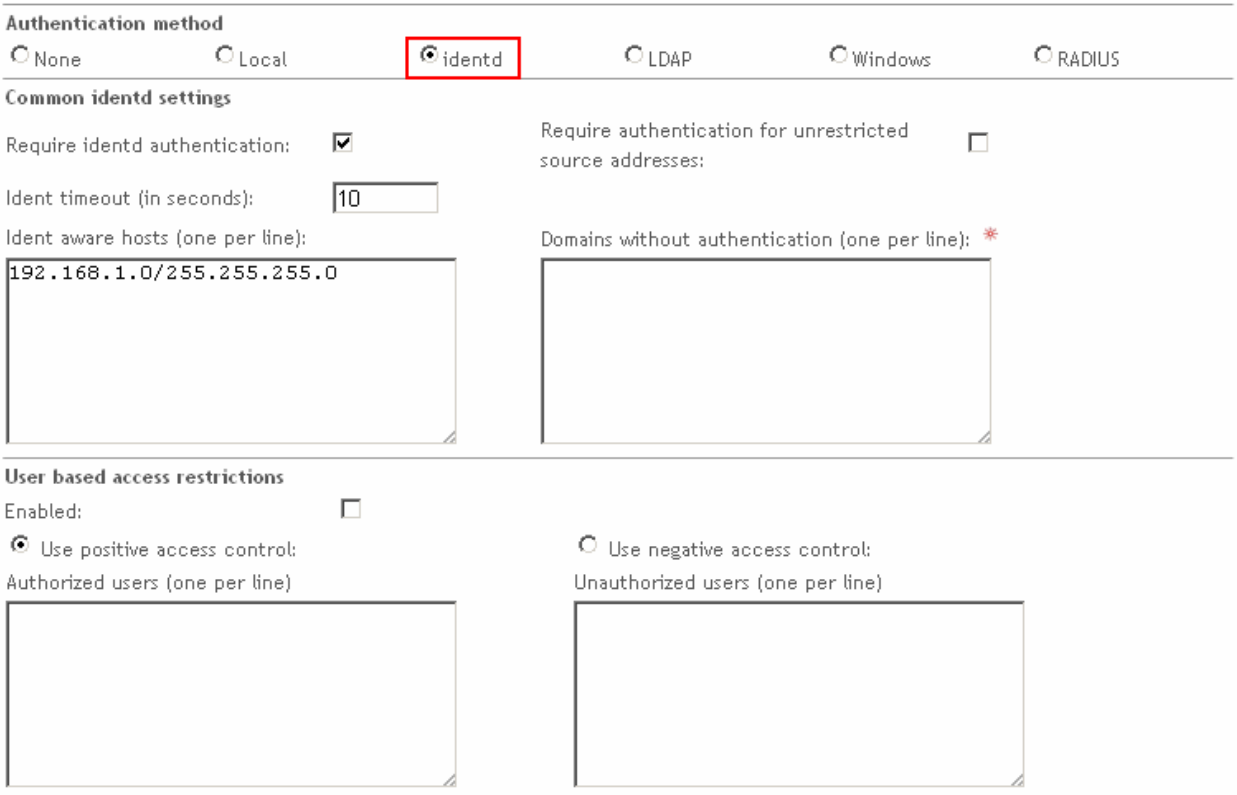
Тепер, якщо користувач захоче зробити запит у якому будуть зустрічатись ключові слова, а також відкрити сторінку де зустрічаються такі слова, з'явиться повідомлення про заборону доступу.
По завершенню формування списку слід зберегти налаштування, натиснувши на **Save and Restart**


Як показало експериментальне використання мережі з сервером IPFIRE, режим блокування за ключовими словами є найефективнішим і найменше «затримує» відгук сервера з контентом.

## 4.2. Режим без авторизації з доступом до певних сайтів

Пункт Authentication method (метод авторизації)

Обираємо метод **Identd,** переходимо до низу сторінки та натискаємо кнопку SAVE. Перед нами з'явиться вікно з активованим методом Identd.



**require identd authentication** ставимо галочку

**identd timeout (in seconds)** вказуємо 10

**identd aware hosts** - 192.168.0.0/24 або 192.168.0.0/255.255.255.0. (для нашої мережі)
**domain without authentication** - перераховуємо дозволені сайти.
**Наприклад:**
Вказуємо домени та під домени

***.advproxy.net;**
***.google.com;**

Окремі сайти

**www.advproxy.net;**
**www.google.com;**

Окремі посилання:

**www.advproxy.net/download**
**www.google.com/images**

Після внесення змін переходимо в кінець сторінки до завершення сторінки та натискаємо **SAVE AND RESTART** – зберегти зміни та перезавантажити проксі-сервер.

## 5. Післямова

Пропоновані рекомендації далеко не повністю вичерпують можливості по організації доступу до мережі Інтернет, що їх може надати система IPFARE 2.9. Але описаних можливостей достатньо для вирішення завдань, що були сформульовані в п.1.
Автори будуть вдячні за висловлені побажання щодо покращення тексту та вказівки на можливі неточності.
***Контакти:***
**Лабораторія Інформаційних та комунікаційних технологій ФМГ№17 м. Вінниці, 21050 м.Вінниця, вул. Інтернаціональна,2**
e-mail **likt@edu.vn.ua** , Skype **pasichov,** ICQ **324249091**
**http://likt.edu.vn.ua , т.(0432)690880**