МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторних робіт з дисципліни
"Комп’ютерні мережі"
для студентів напряму підготовки 6.050102 "Комп'ютерна інженерія",
усіх форм навчання

Перетворення мережевих адрес (NAT). UserGate

2014

Методичні вказівки до виконання лабораторних робіт з дисципліни "Комп’ютерні мережі" для студентів напряму підготовки 6.050102 "Комп'ютерна інженерія", усіх форм навчання. Перетворення мережевих адрес (NAT). UserGate / Укл. Г.Г. Киричек, Т.М. Семерюк. – Запоріжжя: ЗНТУ, 2014. – 46 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.,
Т.М. Семерюк, асистент

Рецензент:

О.І. Вершина, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ

Протокол № 6
від 17.03.2014

ЗМІСТ

1 ЛАБОРАТОРНА РОБОТА №1
Перетворення мережевих адрес (NAT)

Мета роботи – ознайомитись з правилами адресації внутрішніх та завнішних мереж, організувати маршрутизацію з використанням мережевої технології NAT.

1.1 Теоретичні відомості

Трансляція ір NAT, що визначена в RFC 3022, дозволяє вузлу, який не має дійсної, зареєстрованої, глобальної, унікальної IP адреси, здійснювати зв'язок з іншими вузлами через мережі передачі даних. Ці вузли можуть використовувати приватні адреси. Трансляція NAT дозволяє здійснювати зв'язок з вузлами в Інтернет. NAT замінює приватні IP-адреси відкритими зареєстрованими IP-адресами в кожному пакеті протоколу IP. Перетворення мережевих адрес (Network address translation, NAT) реалізовано програмою, вбудованою в маршрутизатор. Ця програма відіграє роль посередника між приватною мережею та Інтернет - серверами із зареєстрованими адресами. Навіть клієнтські комп'ютери з незареєстрованними адресами можуть відправляти запити серверам Інтернету та одержувати від них відповідь за допомогою NAT. Маршрутизатор NAT також змінює поле з адресою відправника у всіх дейтаграмах, отриманих від комп'ютерів з незареєстрованими IP-адресами та підтримує таблицю незареєстрованних адрес приватної мережі, яка необхідна для відстеження оброблених їм дейтаграм.

У мережі можна використовувати два типи IP-адрес: **зовнішні** (**зареєстровані, відкриті**); **внутрішні** (**приватні**).

Якщо мережа не підключена до Інтернету, в ній можна використовувати адреси будь-якого типу, аби тільки дотримувалася їх унікальність. Бажано використовувати один з діапазонів IP-адрес, спеціально виділених для приватних мереж:

- **10.0.0.0 - 10.255.255.255 (10.0.0.0/8) -** одна мережа класу **A.**
- **172.16.0.0 - 172.31.255.255 (172.16.0.0/12) -** група з 16

суміжних мереж класу **B.**

– **192.168.0**.0 - **192.168.255**.255 (**192.168.0.0/16**) - група з 256 суміжних мереж класу C.

Технологія *трансляції мережевих адрес* дозволяє всім вузлам внутрішньої мережі одночасно взаємодіяти із зовнішніми мережами, використовуючи єдину зареєстровану IP-адресу. Ця модель задовольняє вимогам більшості мереж середніх розмірів для доступу до зовнішніх мереж при використанні єдиної зареєстрованої IP-адреси, отриманої від постачальника послуг.

На рисунку 1.1 наведений приклад, коли внутрішня мережа використовує приватну адресу з діапазону **10.0.0.0/8**.

Рисунок 1.1 - Трансляція адрес у технології NAT

Маршрутизатор змінює IP адресу відправника, коли пакет залишає організацію і IP адресу одержувача кожного пакета, який повертається назад у приватну мережу. Функція NAT, яка налаштована на маршрутизаторі, виконує трансляцію адрес.

Коли хост **10.1.1.1** внутрішньої мережі посилає пакет хосту **170.1.1.1** у зовнішню мережу, то він, відправляючи пакет маршрутизатору, як адресу призначення вказує глобальну адресу **170.1.1.1.** Маршрутизатор знає шлях до мережі **170.1.0.0**/16, тому він

передає пакет на зовнішній інтерфейс. При цьому пристрій NAT маршрутизатора транслює адресу джерела **10.1.1.1** у глобально унікальну адресу **200.1.1.1**.

Коли одержувач (хост **170.1.1.1)** генерує відповідне повідомлення, то він як адресу призначення вказує єдину зареєстровану глобальну адресу внутрішньої мережі, яка є адресою зовнішнього інтерфейсу пристрою NAT (у даному прикладі це **200.1.1.1**). При надходженні відповідного пакета на пристрій NAT внутрішньої мережі визначається внутрішня IP-адреса вузла. Ця процедура трансляції повністю прозора для кінцевих вузлів.

1.1.1 Статична трансляція NAT

Статична трансляція NAT - IP-адреси перетворюються один в одну статично (рис.1.2).

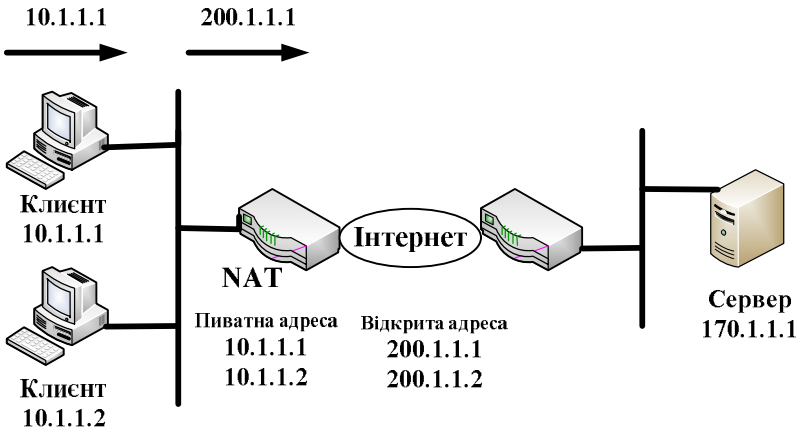

Рисунок 1.2 – Статична трансляція NAT

Розглянемо основні принципи. ISP- провайдер компанії призначає їй зареєстрований номер мережі 200.1.1.0. Маршрутизатор NAT робить так, щоб приватна адреса виглядала таким чином, як ніби віна знаходиться в мережі 200.1.1.0 . Для цього маршрутизатор NAT

змінює IP адресу відправника в пакетах.

У даному прикладі маршрутизатор NAT змінює адресу відправника 10.1.1.1 на адресу 200.1.1.1. При використанні статичної трансляції NAT маршрутизатор просто здійснює взаємно однозначне перетворення між приватною та зареєстрованою адресою, від імені якої він виступає. На маршрутизаторі NAT зроблено статичне перетворення приватної адреси 10.1.1.1 у відкриту зареєстровану адресу 200.1.1.1.

Підтримка двох IP- вузлів у приватній мережі вимагає наступного взаємно однозначного перетворення з використанням другої IP- адреси в діапазоні відкритих адрес. Наприклад, для підтримки адреси 10.1.1.2 маршрутизатор просто перетворює адресу 10.1.1.2 на адресу 200.1.1.2. Оскільки підприємство має одну зареєстровану мережу класу С , використовуючи трансляцію NAT, воно може підтримувати до 254 приватних IP- адрес (при цьому зарезервовані дві звичайні адреси - номер мережі та її широкомовна адреса).

У таблиці NAT приватні IP- адреси наводяться як «приватні», а відкриті, зареєстровані адреси мережі 200.1.1.0 - як «відкриті». Компанія Cisco використовує термін «внутрішні локальні адреси» для приватних IP- адрес і «внутрішні глобальні адреси» для відкритих IP-адрес.

1.1.2 Динамічна трансляція NAT

Динамічна трансляція NAT - маршрутизатор NAT здійснює взаємно однозначне перетворення між внутрішніми локальними і внутрішніми глобальними адресами та змінює IP- адреси в пакетах динамічно.

Динамічна трансляція NAT створює пул можливих внутрішніх глобальних адрес і визначає критерій відповідності для визначення того, які внутрішні глобальні IP- адреси повинні транслюватися за допомогою NAT. Нижче (рис.1.3) встановлено пул з п'яти глобальних IP-адрес в діапазоні 200.1.1.1 - 200.1.1.5. Трансляція NAT налаштована

для трансляції всіх внутрішніх локальних адрес, які починаються з октетів 10.1.1.

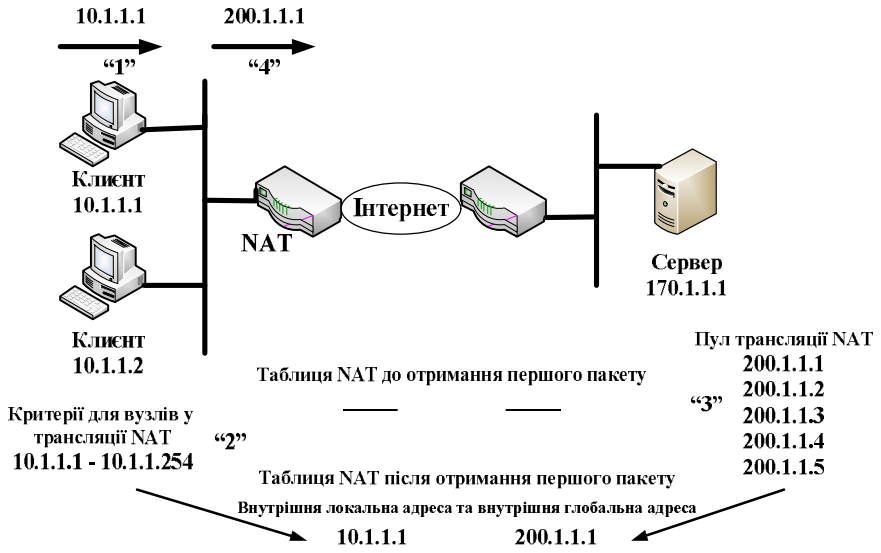

Рисунок 1.3 – Динамічна трансляція NAT

Номери 1, 2, 3 і 4 на рисунку 1.3 відносяться до такої послідовності подій:

– вузол 10.1.1.1 посилає свій перший пакет на сервер, розташований за адресою 170.1.1.1;

– коли пакет поступає на маршрутизатор NAT, маршрутизатор застосовує логіку перевірки відповідності та вирішує, чи слід застосувати до цього пакету трансляцію NAT. Оскільки логіка маршрутизатора налаштована на відповідність IP-адресам відправника, які починаються з 10.1.1 , маршрутизатор додає запис в таблицю NAT для адреси 10.1.1.1 в якості внутрішньої адреси;

– маршрутизатору NAT потрібно виділити IP адресу з пулу дійсних внутрішніх глобальних адрес. Він вибере першу доступну адресу (в даному випадку 200.1.1.1) і додасть її в таблицю NAT для завершення запису;

– маршрутизатор NAT транслює IP адресу відправника і

пересилає пакет.

Динамічний запис залишається в таблиці поки триває передача даних. Можна задати значення тайм- ауту, який визначає, як довго повинен чекати маршрутизатор поки не транслюються пакети з такою адресою, перед видаленням цього динамічного запису.

Трансляція NAT може бути налаштована з великою кількістю IP- адрес у списку внутрішніх локальних адрес, ніж в пулі внутрішніх глобальних адрес. Маршрутизатор виділяє адреси з пулу до тих пір, поки всі вони не будуть виділені.

Якщо надходить новий пакет від ще одного внутрішнього вузла і йому потрібен запис NAT, а всі IP- адреси, які знаходяться в пулі, вже використовуються, то маршрутизатор просто відкидає цей пакет. Користувач повторює спробу до тих пір, поки не закінчиться час тайм-ауту для запису NAT, в цей момент функція NAT працює для наступного вузла, який відправляє пакет.

Розмір внутрішнього глобального пулу адрес повинен відповідати максимальній кількості конкуруючих вузлів, яким потрібен одночасний доступ до мережі інтернет (крім випадку використання трансляції PAT) .

1.2 Організація автономного домену rmf.…domain01. local

Примітка. Методичні вказівки для цієї роботи складені з орієнтацією на виконання роботи на комп'ютерах з фізичними іменами **RMF01**, **RMF02** і **RMF03**.

Для цих комп'ютерів маємо:

– при завантаженні на них клієнтської ОС **MS Windows 7:**

1) IP-адреси: **10.0.9.51, 10.0.9.52** і **10.0.9.53** відповідно;
2) мережеві імена: **rmf51, rmf52** і **rmf53** відповідно;

– при завантаженні на них серверної ОС **Microsoft Windows Server 2008:**

1) IP-адреси: **10.0.9.151, 10.0.9.152** і **10.0.9.153** відповідно;
2) мережеві імена: **rmf151, rmf152** і **rmf153** відповідно;
3) повні імена: **rmf151.domain01.local, rmf152.domain02.local** і **rmf153.domain03.local** відповідно.

Так як більшість з вас працює за комп'ютерами з іншими фізичними іменами, то при виконанні роботи вам доведеться використовувати відповідно інші IP–адреси, короткі і повні мережеві імена.

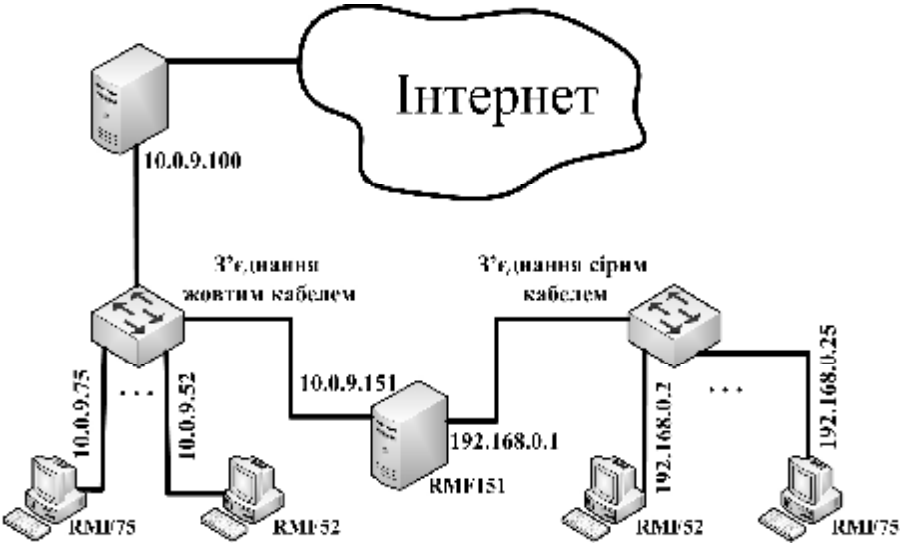

Рисунок 1.4 – Комп'ютерна мережа з підмережею з використанням комутаторів

На рисунку 1.4 наведена комп'ютерна мережа:

– мережа **10.0.9.**0/24 - відповідає з'єднанню **жовтого кабелю** (до складу підмережі включені сервер **(10.0.9.100)** комп'ютери з фізичними іменами **RMF01,** …, **RMF25** і комутатор);

– підмережа **192.168.0.**0/24 - відповідає з'єднанню **сірого кабелю** (до складу підмережі включені комп'ютери з фізичними іменами **RMF01,** …, **RMF25** і комутатор);

– функції маршрутизатора виконує комп'ютер **RMF01** (фізичне ім'я).

IP-адреси комп'ютерів основної мережі, які вказані на рисунку, відповідають завантаженню на комп'ютері з фізичним ім'ям **RMF01** ОС **Microsoft Windows Server 2008**, а на комп'ютерах з фізичними

іменами **RMF02, …, RMF25** - ОС **Microsoft Windows 7**.

На рисунку 1.5 наведена комп'ютерна мережа **10.0.9.**0/24 з підмережею **192.168.0.**0/24, у складі якої всього лише одна робоча станція (**RMF02**).

IP-адреси комп'ютерів основної мережі, які вказані на рисунку, відповідають завантаженню на комп'ютері з фізичним ім'ям **RMF01** ОС **Microsoft Windows Server 2008**, а на комп'ютері з фізичним ім'ям **RMF03** - ОС **Microsoft Windows 7**.

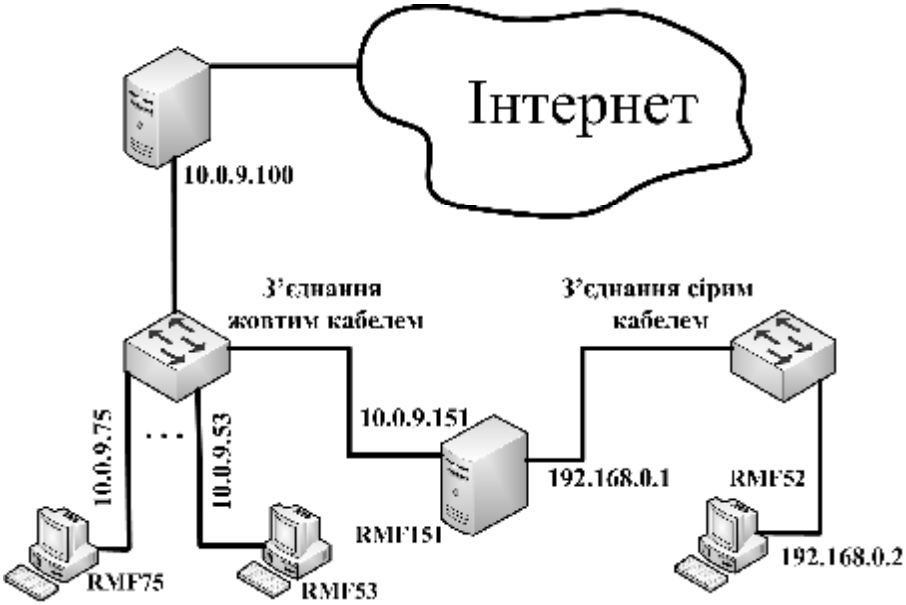

Рисунок 1.5 – Робоча схема мережі

1. Зберіть робочу схему мережі згідно рисунку 1.5:
2. На комп'ютері з фізичним ім'ям **RMF01** виконайте наступні операції:

– завантажте ОС **Microsoft Window Server 2008** (користувач – **Администратор**, Пароль – **1q2w3e4r&** або **1q2w3e4r5t& (RU)**);

– настройте мережевий інтерфейс верхнього адаптера (інтерфейс із підмережею **192.168.0.**0/24):

Пуск => Панель управления => Сеть и интернет (якщо

режим просмотру **Категория)** => **Центр управления сетями и общим доступом**;

– в лівій частині вікна натисніть по **Изменение параметров адаптера** натисніть правою кнопкою миші по **Подключение по локальной сети 2 (сірий кабель)** => виберіть **Свойства** => виділіть **Протокол Интернета версии 4 (TCP/IPv4)** => натисніть **Свойства;**

– установіть наступні параметри:

виберіть опцію **Использовать следующий IP-адрес**

IP-адрес: **192.168.0.1**

Маска подсети: **255.255.255.0**

Основной шлюз: **10.0.9.151** (у вас, відповідно, інша адреса)

Предпочитаемый DNS-сервер: 10.0.9.151 (у вас, відповідно,інша адреса)

натисніть **OK**.

3. Перевірте настроювання мережевого інтерфейсу нижнього адаптера (інтерфейс із мережею **10.0.9.**0/24);

– перебуваючи у вікні **Сетевые подключения**, натисніть правою кнопкою миші **Подключение по локальной сети (жовтий кабель)** => виберіть **Свойства** => виділіть **Протокол Интернета версии 4 (TCP/IPv4)** => натисніть **Свойства;**

– установіть наступні параметри:

IP-адрес: **10.0.9.151** (у вас, відповідно, інша адреса)

Маска подсети: **255.255.255.0**

Основной шлюз: **10.0.9.100**

Предпочитаемый DNS-сервер: 10.0.2.1

і натисніть **OK**.

4. Створіть користувача **Active Directory**:

– **Пуск => Администрирование => Active Directory – пользователи и компьютеры;**

– розкрийте список вузла вашого сервера (якщо він не розкритий);

– натисніть ліворуч правою кнопкою миші по **Users** і виберіть **Создать => Пользователь**;

– у вікні **Новый объект-Пользователь**:

– у полі **Имя** введіть **user1**;

– у полі **Имя входа пользователя** введіть **user1**;

– натисніть **Далее**;

– у вікні **Новый объект-Пользователь**:

– у полі **Пароль** введіть **1q2w3e4r5t&** або **1q2w3e4r& (RU) (**залежно від паролю адміністратора**)**);

– у полі **Подтверждение** введіть **1q2w3e4r5t&** або **1q2w3e4r& (RU)**;

– установіть прапорець **Запретить смену пароля пользователем**;

– установіть прапорець **Срок действия пароля не ограничен**;

– натисніть **Далее**;

– натисніть **Готово**;

– закрийте вікно **Active Directory – пользователи и компьютеры**.

5. На комп'ютері з фізичним ім'ям **RMF02** виконайте наступні дії:

– завантажте ОС **Microsoft Windows 7** (Користувач – **admin**, Пароль – **1234567**);

– настройте мережевий інтерфейс:

Пуск => Панель управления => Сеть и интернет (якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**;

– в лівій частині вікна натисніть по **Изменение параметров адаптера** натисніть правою кнопкою миші по **Подключение по локальной сети 2 (сірий кабель) =>** виберіть **Свойства =>** виділіть **Протокол Интернета версии 4 (TCP/IPv4) =>** натисніть **Свойства;**

– установіть наступні параметри:

виберіть опцію **Использовать следующий IP-адрес**

IP-адрес: **192.168.0.2**

Маска подсети: **255.255.255.0**

Основной шлюз: **192.168.0.1**

Предпочитаемый DNS-сервер: 192.168.0.1 (10.0.2.1) (у вас, відповідно,інша адреса) і натисніть **OK**,

– закрийте вікно **Сетевые подключения.**

6. Підключіть комп'ютер з мережевим ім'ям **rmf52** до домену **domain01.local**, тобто до домену, у котрому контролером домену є комп'ютер з фізичним ім'ям **RMF01**:

– **Мой компьютер** (правою кнопкою миші) **=> Свойства =>**

у розділі **Имя компьютера, имя домена и параметры рабочей группы** натисніть **Изменить параметры** => натисніть кнопку **Изменить…;**

– у вікні **Изменение имени компьютера или домена** виберіть опцію **Является членом домена**, у текстовому полі впишіть **domain01.local** (у вас, відповідно, інше ім'я домена)**,** натисніть **ОК,**

– у вікні **Имя и пароль пользователя в домене**:

1) у полі **Пользователь** введіть **Администратор**;
2) у полі **Пароль** введіть **1q2w3e4r&** або **1q2w3e4r5t& (RU)**;

– натисніть **ОК;**

– через деякий час відкриється вікно з запрошенням в домен **domain01.local**, натисніть **ОК;**

– погодьтеся з пропозицією перезавантажити комп'ютер, клацнувши **ОК** (при цьому ви вертаєтеся у вікно **Свойства системы**), натисніть **Закрыть**, потім – **Да;**

– після перезавантаження комп'ютера (не забудьте перевести курсор на рядок **Microsoft Windows 7**) виконайте вхід в систему **за трьома параметрами:**

Користувач – **user1**;

Пароль – **1q2w3e4r5t&** або **1q2w3e4r& (RU)**;

Вхід в – **DOMAIN01** (у вас, відповідно, буде “своє” ім'я домену).

1.3 Настроювання NAT-серверу та перевірка його працездатності

1. На комп'ютері з фізичним ім'ям **RMF01** виконайте наступні операції:

– запустіть службу **Брандмауэр Windows;**

– **пуск => Администрирование => Службы;**

– в правій частині натисніть правою кнопкою миші по пункту **Брандмауэр Windows => Свойства;**

– встановіть **Тип запуска => Авто;**

– якщо служба ще не запущена, запустіть її – натисніть на кнопку **=> Запустить;**

– натисніть => **ОК;**

– закрийте вікно => **Службы;**

– добавте роль => **Службы политики сети и доступа;**

– **пуск => Администрирование => Диспетчер сервера;**

– в лівій частині вікна виберіть пункт **Роли;**

– в правій частині вікна натисніть => **Добавить роли,** відкриється **Мастер добавления ролей;**

– якщо першою сторінкою є **Перед началом работы**, пропускаємо її, натисніть **Далее;**

– на сторінці **Роли сервера** встановіть прапорець **Службы политики сети и доступа => Далее;**

– пропускаємо сторінку **Службы политики сети и доступа**, натисніть **Далее;**

– на сторінці **Службы ролей** встановіть прапорець **Службы маршрутизации и удаленного доступа => Далее;**

– підтвердить обрані налаштування, натисніть **Установить;**

– по завершенні установки натисніть **Закрыть;**

– закрийте вікно **Диспетчер сервера.**

Запустіть службу Маршрутизация и удаленный доступ:

– **пуск => Администрирование => Маршрутизация и удаленный доступ;**

– на лівій панелі виділіть рядок **Состояние сервера.** Праворуч відобразиться його статус**: зупинений або запущений. Якщо він зупинений (на його значку присутня червона стрілка), то натисніть на ньому (на записі RMF151 (локально)) правою кнопкою миші й виберіть Настроить и включить маршрутизацию и удаленный доступ;**

– натисніть **Далее;**

– у вікні **Конфигурация** виберіть опцію **Преобразование сетевых адресов (NAT)** і натисніть **Далее;**

– у вікні **Подключение к Интернету на основе NAT** виберіть опцію **Использовать общедоступный интерфейс для подключения к Интернету** та оберіть мережевий інтерфейс **Внешняя сеть,** натисніть **Далее;**

– натисніть **Готово;**

– закрийте вікно **Маршрутизация и удаленный доступ.**

2. Перевірте мережеві підключення за допомогою команди **ping**:

– на комп'ютері **RMF02** виконайте **Пуск => Все программы => Стандартные => Командная строка;**

– виконайте команди **ping 192.168.0.1 і ping 10.0.9.151 (у вас, відповідно, інша адреса). Обидві команди повинні виконатися коректно (Пакетов: отправлено = 4, получено = 4, потеряно = 0);**

– закрийте вікно **Командная строка**.

3. Перевірте працездатність протоколу NAT за допомогою мережевого монітора:

– на комп'ютері **RMF01** установіть мережевий монітор**:**

– **пуск => Все программы => Стандартные => Выполнить;**

– у рядку **Открыть** введіть**: "C:\Install\NetworkMonitor \NM32_x86.exe" та натисніть ОК;**

– натисніть **Да;**

– натисніть **Next;**

– погоджуйтесь із ліцензійним погодженням, оберіть **I accept the terms in the License Agreement,** натисніть **Next;**

– оберіть пункт **I do not want to use Microsoft Update, натисніть Next;**

– натисніть **Typical;**

– натисніть **Install;**

– по завершенні установки натисніть **Finish.**

4. Виконайте перехоплення кадрів:

– **на комп'ютері RMF03:**

– завантажте ОС Windows 7 (Користувач – **admin**, Пароль – **1234567**);

– перевірте настроювання мережевого інтерфейсу, воно повинно бути наступним:

IP-адрес: **10.0.9.53** (у вас, відповідно, інша адреса)

Маска подсети: **255.255.255.0**

Основной шлюз: **10.0.9.100**

Предпочитаемый DNS-сервер: 10.0.2.1

– створіть спільний мережевий ресурс:

– **Мой компьютер** => **диск С** => **папка TEMP** (при її відсутності - **створіть**);

– скопіюйте в папку **C:\TEMP** будь-який файл невеликого розміру;

– натисніть правою клавішею миші на папці **C:\TEMP** і виберіть **Общий доступ => Конкретные пользователи;**

– у верхньому рядку оберіть варіант **Все**, натисніть **Добавить**;

– натисніть => **Общий доступ;**

– натисніть => **Готово.**

5. На комп'ютері **RMF01** визначте фізичну адресу **мережевого адаптера для зовнішньої мережі**:

– **Пуск => Выполнить;**

– у полі **Открыть** впишіть **cmd** і натисніть **ОК;**

– у вікні, яке відкрилося, виконайте команду **ipconfig /all;**

– прочитайте фізичну адресу адаптера для **Подключение по локальной сети** і запишіть її;

– закрийте вікно **F:\SERVER\System32\cmd.exe**;

– на комп'ютері **RMF01** запустіть процес перехоплення кадрів:

– **Пуск => Все программы => Microsoft Network Monitor 3.4 => Microsoft Network Monitor 3.4**;

– якщо відкрилося вікно **Microsoft Update Opt-In**, то зніміть прапорець **Periodically check for updates when Network Monitor starts,** та натисніть **No;**

– натисніть **File => New => Capture;**

– натисніть **Capture => Start.**

6. З комп'ютера **RMF02** (фізичне ім’я) запросіть інформацію на комп'ютері **RMF03** (фізичне ім’я):

– **Пуск => Все программы => Стандартные => Выполнить;**

– у полі **Открыть** впишіть **\\10.0.9.53\temp** (у вас, відповідно, інша адреса) і натисніть **ОК;**

– з вікна **temp на 10.0.9.53** скопіюйте файл **GHOSTERR або інший** на робочий стіл комп'ютера; це запустить трафік у мережі, який і буде перехоплений мережним монітором;

– закрийте вікно **temp на 10.0.9.53**;

– на комп'ютері **RMF01** (фізичне ім’я) зупиніть процес перехоплення кадрів (**Capture => Stop**);

– на комп'ютері **RMF01** (фізичне ім’я) перегляньте перехоплені дані, які перебувають у буфері;

– перелік перехоплених кадрів можна побачити у вікні **Frame Summary**;

– для перегляду вмісту окремого кадру натисніть мишею на будь-якому (можна першому в переліку) кадрі, де адреса відправника (див. колонку **Source**) дорівнює IP-адресі комп'ютера **RMF03** (тобто **10.0.9.53**; у вас, відповідно, інша адреса);

– у вікні Frame Details розкрийте значок **+** поруч із назвою протоколу IPv4 і знайдіть у заголовку дейтаграми поле з адресою відправника (**Source Address**) і поле з адресою одержувача (**Destination Address**), запишіть ці адреси (це будуть наступні адреси: **10.0.9.53** і **10.0.9.151**; у вас, відповідно, "свої");

– розкрийте значок **+** поруч із назвою протоколу TCP і знайдіть у заголовку сегмента TCP поле с номером порту відправника (**SrcPort**) і поле з номером порту одержувача (**DstPort**), запишіть ці номери портів;

– **переконайтесь** що комп'ютер **RMF03** не знає IP- адресу комп'ютера **RMF02**, який знаходиться в підмережі, а знає тільки IP-адресу та порт комп'ютера **RMF01** (тобто **10.0.9.151**; у вас, відповідно, інша адреса), якому він і пересилав кадри. Служба NAT на комп'ютері **RMF01** виконувала пересилання кадрів на комп'ютер **RMF02** (структура внутрішньої мережі (**192.168.0.**0/24) від комп'ютерів у зовнішній мережі схована);

– закрийте значок "мінус" (**-**) поруч с назвою протоколу TCP;

– закрийте значок "мінус" (**-**) поруч с назвою протоколу IPv4;

– закрийте вікно **Microsoft Network Monitor 3.4 …** (без збереження зібраних даних і без збереження бази даних адрес).

1.4 Відновлення комп'ютерів в початковий стан

(даний розділ підлягає обов'язковому виконанню!)

1. На комп'ютері з фізичним ім'ям **RMF03** виконайте наступні дії:

– видаліть з папки **C:\TEMP** файл;

– зніміть спільний доступ до папки **C:\TEMP:**

1) натисніть правою клавішею миші на папці **C:\TEMP**,

виберіть **Свойства;**

2) у вікні **Свойства** перейдіть до вкладки **Доступ,** натисніть **Расширенная настройка**, зніміть прапорець **Открыть общий доступ к этой папке**, клаціть **ОК** потім **Закрыть;**

– закрийте вікно **С;**

– перезавантажте комп'ютер із завантаженням ОС, яка установлюється за замовчуванням.

2. На комп'ютері з фізичним ім'ям **RMF02** виконайте наступні дії:

– видаліть з робочого стола комп'ютера файл **GHOSTERR** (або інший, який був скопійований з комп'ютера **RMF03**);

– відключіть цей комп'ютер від домену **domain01.local**:

Мой компьютер (правою кнопкою миші) => **Свойства** => у розділі **Имя компьютера, имя домена и параметры рабочей группы** натисніть => **Изменить параметры** => натисніть кнопку **Изменить**…;

– у вікні => **Изменение имени компьютера или домена**:

1) виберіть опцію => **Является членом рабочей группы**;

2) у текстовому полі впишіть **WORKGROUP**;

3) натисніть **Дополнительно**;

4) у вікні **DNS–суффикс и NetBIOS–имя компьютера** у текстовому полі видаліть DNS–суфікс **domain01.local** (у вас, відповідно, "свій" DNS– суфікс), зробіть чистим текстове поле, і натисніть => **ОК**;

5) с поверненням у вікно => **Изменение имени компьютера или домена** натисніть => **ОК**;

– через деякий час відкриється вікно **Сетевая идентификация** з запрошенням в робочу групу, натисніть => **ОК**;

– погодьтеся з пропозицією перезавантажити комп'ютер, клацнувши => **ОК**;

– у вікні **Свойства системы** натисніть => **ОК**.

Важливо!!! Якщо вікно **Изменение имени компьютера или домена** не є активним, змініть Користувача:

– у полі **Пользователь** введіть:

DOMAIN01\Администратор (у вас, відповідно, буде "своє" ім'я домену);

– у полі **Пароль** введіть **1q2w3e4r&** або **1q2w3e4r5t& (RU)**;

– натисніть **ОК;**

– потім виконайте відключення від домену **domain01.local.**

3. Перевірте, що комп'ютер з фізичним ім'ям **RMF02** відключено від домену **domain01.local**.

– після перезавантаження комп'ютера (не забудьте перевести курсор на рядок **Microsoft Windows 7**) виконайте вхід в систему за двома параметрами:

Користувач – **admin**;

Пароль – **1234567**. **Да;**

– відновіть початковий стан мережевого інтерфейсу (верхньої мережевої плати);

– **Пуск** => **Панель управления** => **Сеть и интернет** (якщо режим просмотру **Категория**) => **Центр управления сетями и общим доступом**;

– в лівій частині вікна натисніть => **Изменение параметров адаптера** натисніть правою кнопкою миші => **Подключение по локальной сети 2** => виберіть **Свойства** => виділіть **Протокол Интернета (TCP/IP)** => натисніть **Свойства**;

– установіть опції => **Получить IP–адрес автоматически і Получить адрес DNS–сервера автоматически** і натисніть => **ОК**;

– з поверненням у вікно **Подключение по локальной сети** => **Свойства** натисніть => **ОК**;

– з поверненням у вікно **Сетевые подключения** закрийте його;

– перезавантажте комп'ютер із завантаженням ОС, яка установлюється за замовчуванням.

4. На комп'ютері з фізичним ім'ям **RMF01** виконайте наступні дії:

– відновіть настроювання мережевого інтерфейсу верхнього адаптера (**сірий кабель**)**:**

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом;**

– в лівій частині вікна натисніть **=> Изменение параметров адаптера** натисніть правою кнопкою миші **=> Подключение по локальной сети 2** => виберіть **Свойства** => виділіть **Протокол Интернета (TCP/IP)** => натисніть **Свойства;**

– установіть опції**:**

Получить IP–адрес автоматически і Получить адрес DNS–сервера автоматически і натисніть => **ОК;**

– натисніть **ОК;**

– закрийте вікно **Сеть и удаленный доступ к сети;**

– видаліть **роль Службы политики сети и доступа**:

1) **Пуск => Администрирование => Диспетчер сервера;**

2) на лівій панелі натисніть правою кнопкою миші => **Роли;**

3) у вікні => **Роли** натисніть => **Удалить роли**;

4) якщо першою сторінкою майстра є => **Перед началом работы**, натисніть => **Далее;**

5) У вікні => **Удаление ролей сервера** зніміть прапорець => **Службы политики сети и доступа;**

6) натисніть **Далее;**

7) натисніть **Удалить;**

5. Видаліть мережевий монітор:

– **Пуск** => **Панель управления** => **Программы и компоненты**;

– у вікні **Программы и компоненты** => виділить **Microsoft Network Monitor 3.4** і => натисніть **Удалить**;

– натисніть **Да;**

– закрийте вікно **Программы и компоненты**;

– закрийте вікно **Панель управления**.

6. Видаліть реєстраційний запис комп'ютера **RMF02** у домені **domain01.local**:

– **Пуск** => **Администрирование** => **Active Directory – пользователи и компьютеры**;

– с відкриттям вікна **Active Directory – пользователи и компьютеры** натисніть на значку + у рядку **domain01.local** (у вас, відповідно, “своє” ім'я);

– виділіть **Computers**;

– на полі праворуч натисніть правою кнопкою миші на записі **rmf52** Компьютер (у вас, відповідно, аналогічний запис) і виберіть **Удалить**, потім – **Да**;

– закрийте вікно **Active Directory – пользователи и компьютеры**;

– перезавантажте комп'ютер із завантаженням ОС, яка

установлюється за замовчуванням.

1.5 Зміст письмового звіту

1. Теоретичні відомості.
2. Загальні схеми.
3. Хід роботи.
4. Відповіді на контрольні питання.

1.6 Контрольні питання

1. Причини використання технології NAT?
2. Пули IP-адрес, які зарезервовані для адресації в приватних мережах?
3. Статична трансляція NAT. Приклад.
4. Динамічна трансляція NAT. Приклад.

2 ЛАБОРАТОРНА РОБОТА №2

Захист мережі за допомогою брадмауера.UserGate

Мета роботи – навчитися використовувати утиліту UserGate для налаштування загального доступу в Інтернет з локальної мережі**.**

2.1 Загальні відомості

Програмне забезпечення UserGate є комплексним рішенням для організації загального доступу в Інтернет з локальної мережі, обліку трафіка і захисту корпоративної мережі від зовнішніх загроз. Продукт UserGate - ефективна альтернатива дорогому програмному і апаратному забезпеченню, що призначено для використання в компаніях малого і середнього бізнесу.

На даний час, коли мережі Інтернет використовує абсолютна більшості організацій, виникає завдання пошуку оптимального способу підключення локальної мережі підприємства до Інтернет.

Найпростіший спосіб - придбати маршрутизатор, як окремий пристрій, який підключається між локальною мережею та Інтернет. Маршрутизатор недорогий і простий в експлуатації пристрій, який можна налаштувати менш ніж за годину при наявності відповідних навичок. Відразу виникає ряд питань: наскільки захищеною буде локальна мережа? Який трафік витрачається кожним з комп'ютерів за певний час? Як виявити використання Інтернет в особистих цілях і блокувати небажані ресурси та розділити трафік різних користувачів, відповідно до пріоритету та більш пріоритетні запити пропускати в першу чергу? Використовувати для цих завдань звичайний маршрутизатор недостатньо. Можливо, знадобиться придбати більш дорогу модель, яка допоможе вирішити деякі з перерахованих завдань.

В якості альтернативи апаратному маршрутизатору можна використовувати утиліту UserGate, яка відноситься до програмних маршрутизаторів. UserGate працює під ОС Windows та встановлюється на комп'ютері, який підключений з одного боку до Інтернет-провайдера, а з іншого - до локальної мережі підприємства.

В якості сервера може виступати і звичайна робоча станція, що особливо актуально в умовах обмеженого бюджету. При цьому функціональність UserGate не поступається функціональності дорогих апаратних маршрутизаторів, в той час поки загальна вартість рішення, що складається з вартості програми та вартості комп'ютера з ОС Windows, в декілька разів нижче. Робота UserGate заснована на використанні облікових записів і правил, які до них застосовуються. Тому ті користувачі в локальній мережі, яких не додано у UserGate у вигляді окремого облікового запису, не зможуть отримати доступ в Інтернет. Це надає адміністратору повний контроль над тим, як витрачається трафік і які ресурси відвідуються співробітниками компанії. Гнучка система правил дозволяє заборонити або обмежити доступ до тих чи інших ресурсів, встановити максимальний обсяг вхідного або вихідного трафіка, а також вести детальну статистику по кожному з користувачів.

Основні функції UserGate: подвійний антивірусний захист; міжмережевий екран; розширений драйвер NAT; підтримка VPN-з'єднань; організація доступу в Інтернет; фільтрація веб-сайтів; контроль додатків; обмеження трафіку і швидкості доступу; облік трафіка; модуль веб-статистики; білінгова система; проксі - сервери для різних протоколів; робота з декількома провайдерами; управління шириною канала; кешурування трафіка; підтримка IP - телефонії; DHCP - сервер; маршрутизація; публікація ресурсів; віддалене адміністрування; високий рівень безпеки; дружній інтерфейс; докладна статистика; безкоштовна фільтрація веб - сайтів на 1 рік; не вимагає спеціального обладнання; доступна ціна.

2.1.1 Організація доступу в Інтернет

UserGate надає користувачам локальної мережі доступ в Інтернет, а адміністраторам - можливість контролювати трафік за допомогою гнучкої системи правил. Доступ в Інтернет може бути організований як через NAT, так і через проксі-сервер для протоколів високого рівня, наприклад**,** HTTP (HTTP-проксі).

Доступ до Інтернету. UserGate являється проміжною ланкою між локальною мережею та мережею Інтернет, дозволяючи

користувачам підключатися до Інтернету під однією і тією ж зовнішнею IP-адресою. При цьому тип Інтернет-підключення може бути будь-яким - DSL, ISDN, комутованим доступом і т.п.

Проксі-сервери. UserGate може працювати як проксі-сервер рівня протоколів додатків, таких як HTTP, FTP, SOCKS, POP3, SMTP, SIP та H.323. При цьому доступний «прозорий» режим роботи проксі, при якому адміністратору нетреба змінювати налаштування доступу на робочих станціях. Адміністратор також може вказати мережеві інтерфейси, для яких використовуватиметься проксі-сервер.

Робота з декількома провайдерами. UserGate дозволяє використовувати декілька інтернет-підключень різних провайдерів.

Якщо основне підключення не працює, то програма автоматично перемкне користувачів на резервне підключення. Крім того, адміністратор має можливість надати доступ до Інтернету для однієї групи користувачів через одного провайдера, а для другої групи користувачів - через іншого.

Управління шириною каналу. Ця функція дозволяє адміністраторові обмежувати швидкість доступу і встановлювати пріоритет обробки IP-пакетів згідно створеним правилам.

Кешірування трафіка. Кешірування файлів відвіданих сторінок звільняє канал для завантаження корисної інформації і економить вхідний трафік.

Підтримка IP-телефонії. Підтримка протоколів SIP і H.323 дозволяє використовувати проксі-сервер UserGate в якості VoIP-шлюзу як для програмних, так і для апаратних IP-телефонів.

2.1.2 Информаційна безпека

UserGate використовує комплексний підхід до підтримки функцій безпеки локальної мережі та сучасних методів боротьби з поширеними інтернет-загрозами, такими, як віруси, шкідливі програми і хакерські атаки.

Захист від вірусів. Питання "Яку антивірусну програму вибрати?" - найбільш часто задається на форумах, присвячених безпеці в Інтернеті. Компанія Entensys співпрацює з двома світовими лідерами в галузі розробки антивірусного ПО «Лабораторією

Касперського» і Panda Security - з метою надання своїм користувачам вибіру антивірусного рішення для використання в складі UserGate. Користувачі можуть за бажанням використовувати той або інший антивірусний модуль, або активувати обидва модулі з метою максимального захисту. При цьому можна комбінувати антивірусний захист UserGate із захистом файлової системи на локальних машинах за допомогою третього антивірусного рішення.

Міжмережевий екран. Міжмережевий екран (брандмауер) в UserGate дозволяє захистити локальну мережу від несанкціонованого доступу ззовні, одночасно надаючи можливість відкрити доступ до внутрішніх ресурсів, таких як поштовий, веб- або VPN-сервер в локальній мережі.

Розширений драйвер NAT. Версія UserGate5 містить новий, розширений варіант драйвера NAT. Функція маршрутизації тепер дозволяє адміністратору створювати локальні підмережі і налаштовувати обмін пакетами між ними. Наявність підтримки протоколів IP-телефонії та публікація ресурсів дозволяють використовувати сучасні способи комунікації та спільної роботи.

Подтримка VPN. VPN - «віртуальна приватна мережа» або шлях, за допомогою якого можна організувати віддалений захищений доступ через відкриті канали Інтернету до серверів баз даних, FTP і поштових серверів. Фізична сутність технології VPN полягає в здатності захистити трафік будь-яких інформаційних інтранет- і екстранет-систем, аудіовідеоконференцій, систем електронної комерції. UserGate підтримує передачу трафіка через протоколи PPTP і L2TP для з'єднання VPN-сервера з VPN-клієнтами локальної мережі.

Крім того, можна використовувати публікацію мережевих ресурсів, щоб зробити VPN-сервер локальної мережі доступним віддалено.

2.1.3 Здійснення контролю доступу

За допомогою UserGate можна контролювати доступ до Інтернету окремих співробітників компанії, а також їх груп, об'єднаних за спільною ознакою.

Користувачі і групи. В основі роботи UserGate перебуває поняття «користувач». Воно може включати комп'ютер або групу комп'ютерів, об'єднаних загальною ознакою, наприклад, IP-адресою або MAC-адресою, логіном і паролем і т.д. Всього в UserGate використовується 8 ознак, згідно з якими проводиться авторизація. Доступ до Інтернету через UserGate можуть отримати тільки авторизовані користувачі.

Фільтрація веб-сайтів. UserGate включає модуль фільтрації сайтів BrightCloud, в базі даних якого міститься > 450 млн. сайтів у 70 категоріях. Адміністратор може забороняти доступ за категоріями, окремими сайтами або фрагментами слів, які є в адресах сайтів.

Контроль додатків. UserGate містить модуль контролю (фільтрації) активності додатків, запущених на комп'ютерах у локальній мережі. Для роботи модуля на всіх клієнтських машинах необхідно встановити безкоштовний клієнтський компонент. Останній буде зв'язуватися з сервером UserGate і блокувати інтернет-програми (наприклад, ICQ або MSN) на локальній машині на основі політик, визначених адміністратором.

Обмеження трафику і швидкості доступу. В прокси-сервері UserGate реалізована розвинена система обмежень трафіку і швидкості доступу для кожного користувача або групи користувачів. Обмеження можуть застосовуватися до різних об'єктів: мережевий адаптер, протокол (TCP, UDP), IP-адреса і порт.

Врахування трафику. UserGate надає адміністраторам повну статистику про відвідуваність ресурсів користувачами , на основі якої можуть бути прийняті рішення про обмеження доступу до ресурсів.

Модуль веб-статистики. Модуль дозволяє отримати доступ до статистики UserGate з точки світу, де існує вихід в мережу Інтернет. Інформація відображається не тільки в табличному вигляді, але і в графічній формі, що суттєво полегшує сприйняття звітів. Об'єм доступної статистичної інформації залежить від рівня доступу - користувач або адміністратор.

Білінгова система. Вбудована білінгова система автоматично проводить розрахунок вартості роботи користувача в мережі Інтернет, на основі ціни, часу і/або обсягу трафіку. Можна встановлювати тарифи окремо для кожного користувача або для групи користувачів. Є можливість зміни тарифів залежно від часу доби, дня тижня або адреси сайту.

2.1.4 Мережеве адміністрування

Наявність в UserGate функцій для виконання деяких рутинних операцій дозволяє спростити мережеве адміністрування.

DHCP-сервер. Вбудований DHCP-сервер автоматизує процес видачі IP-адрес комп'ютерам та іншим пристроям у локальній мережі. Всякий раз при підключенні нового пристрою або відключенні його від мережі, DHCP-сервер оновлює динамічну таблицю виданих IP-адрес у відповідності з умовами та обмеженнями, які визначаються адміністратором.

Маршрутизація. Якщо комп'ютер з UserGate підключений до декількох локальних мереж, сервер UserGate можна налаштувати як маршрутизатор (router), забезпечивши прозорий двунаправлений зв'язок між локальними мережами.

Публікація ресурсів. За допомогою брандмауера в UserGate можна надати доступ до внутрішніх ресурсів підприємства, наприклад, до Web, FTP, VPN або до поштового сервера. У цьому випадку всі звернення на визначений порт зовнішньої IP-адреси комп'ютера з UserGate будуть переадресовані на внутрішній сервер відповідно до створеного правила.

Віддалене адміністрування. До сервера можна підключатися віддалено по локальній мережі або через Інтернет з будь-якого комп'ютера, на якому встановлена Консоль адміністрування UserGate.

2.2 Виконання роботи

2.2.1 Налаштування мережі на сервері

Методичні вказівки складені з орієнтацією виконання роботи на комп’ютерах з фізичними іменами **RMF01** і **RMF02**.

На комп’ютері з фізичним ім’ям **RMF01** виконати наступні дії:

– завантажте ОС **Microsoft Windows 2008 Server RUS** (Користувач – **Администратор**, Пароль – **1q2w3e4r&** або **1q2w3e4r5t&**) (для значка **&** натисніть комбінацію клавіш **Shift+7**).

Примітка. Перед введенням паролю обов'язково перевірьте, який розклад клавіатури встановлений **(встановіть російський розклад клавіатури);**

– налаштуйте мережевий інтерфейс верхнього (сірий кабель) адаптера (інтерфейс з підмережею **192.168.0.**0/24): **Пуск => Панель управления => Сеть и интернет => Центр управления сетями и общим доступом => Изменение параметров адаптера;**

– натисніть правою кнопкою миші **Подключение по локальной сети 2** => виберіть **Свойства** => виділіть **Протокол Интернета (TCP/IPv4)** => натисніть **Свойства;**

– у вікні **Подключение по локальной сети 2** видаліть галочку **Протокол Интернета (TCP/IP v6);**

– встановіть наступні параметри:

виберіть опцію **Использовать следующий IP-адрес**

IP-адрес: **192.168.0.151** (у вас, відповідно, інша адреса, **фізичне ім'я + 150**)

Маска подсети: **255.255.255.0**

Основной шлюз: (зробіть чистим)

Предпочитаемый DNS-сервер: (зробіть чистим)

– натисніть **ОК** і натисніть **Закрыть;**

Перевірте налаштування мережевого інтерфейсу нижнього (жовтий кабель) адаптера (інтерфейс з підмережею **10.0.9.**0/24):

– знаходячись у вікні **Сетевые подключения**, натисніть правою кнопкою миші **Подключение по локальной сети** => виберіть **Свойства =>** виділіть **Протокол Интернета (TCP/IP v4)** => натисніть **Свойства**;

– встановіть наступні параметри:

IP-адрес: **10.0.9.151** (у вас, відповідно, інша адреса)

Маска подсети: **255.255.255.0**

Основной шлюз: **10.0.9.100**

Предпочитаемый DNS-сервер: **10.0.2.1**

– і натисніть **ОК**;

– закрийте вікно **Центр управления сетями и общим доступом.**

2.2.2 Створення доменного облікового запису користувача

Створить і включіть в локальну групу домену обліковий запис користувача**.**

Запустіть на контролері домена: **Пуск => Администрирование => Active Directory-пользователи и компьютеры.**

У вікні **Active Derectory-пользователи и компьютеры** встановіть курсор на **domain01.local => Builtin** (на вашому комп'ютері DNS-ім'я домену буде, відповідно, іншим).

В меню **Действие** виберіть **Создать => Группа.**

У вікні **Новый объект - Группа:**

– в полі **Имя группы** впишіть **ім'я групи - gr_login**, де **login-ім'я користувача** (наприклад, **gr_petrov**);

– в розділі **Область действия группы** виберіть опцію **Локальная в домене**;

– в розділі **Тип группы** виберіть опцію **Группа безопасности**;

– натисніть **ОК** (при цьому у списку основних вбудованих груп з'явиться створена вами група).

– в меню **Действие** виберіть **Создать => Пользователь**;

– в вікні **Новый объект - Пользователь**:

1) в полі **Имя** впишіть **ім'я користувача** (наприклад **petrov**);

2) в полі **Имя входа пользователя** впишіть **ім'я користувача** (наприклад **petrov**) **=> Далее;**

3) в полі **Пароль** введіть пароль користувача (**1q2w3e4r5t&**) (для **&**-shift+7);

4) в полі **Потверждение** введіть підтвердження пароля користувача (**1q2w3e4r5t&**) (для **&**-shift+7);

5) встановіть галочку **Срок действия пароля не ограничен**;

6) прибрати галочку **Требовать смену пароля при следующем входе в систему;**

7) натисніть **Далее;**

8) натисніть **Готово** (при цьому у списку основних вбудованих груп з'явиться створений Вами доменний обліковий запис користувача).

Додайте створений обліковий запис користувача **Petrov** в локальну групу домена **Операторы архива**, щоб користувач міг увійти локально на комп'ютер, для чого:

– натисніть правою кнопкою миші на **gr_petrov** і в контексному меню, що з'явилося, виберіть **Свойства;**

– у вікні **свойства:gr_petrov** перейдіть на вкладку **Члены группы** => натисніть **Добавить;**

– у вікні **Выбор: Пользователи, Контакты, Компьютеры или Группы** натисніть **Дополнительно => Поиск** і встановіть курсор на рядок **petrov domain01.local** => натисніть **ОК;**

– натисніть **ОК** (при цьому у списку **Члены группы** вікна **Свойства: gr_petrov** з'явиться ваш запис **(petrov domain01.local/Builtin**);

– натисніть **Применить** і **ОК.**

2.3 Налаштування мережі на клієнті (RMF02 ,…, RMF25)

Виконайте наступні дії:

– завантажте ОС **Microsoft Windows 7** (користувач – **admin**, пароль – **1234567).** Налаштуйте мережевий інтерфейс верхнього адаптера (підмережа **192.168.0**.0/24):

– в трее натисніть лівою клавишею миші на **Центр управления сетями и общим доступом:**

– у вікні **Центр управления сетями и общим доступом** натисніть правою кнопкою миші **Подключение по локальной сети 2 =>** виберіть **Свойства =>** виділіть **Протокол Интернета ((TCP/IP v4))** => натисніть **Свойства,**

- встановіть наступні параметри:

виберіть опцію **Использовать следующий IP-адрес**

IP-адрес: **192.168.0.52 (**4 байт згідно з **фізичним ім'ям ПК+50** - для **RMF03 (192.168.0.53))**

Маска подсети: **255.255.255.0**

Основной шлюз: **192.168.0.151 (**Подключение по локальной сети 2 **(на сервері)** - для **RMF25 (192.168.0.175))**

Предпочитаемый DNS: **192.168.0.151** (**сервер** - у вас відповідно, інша адреса)

Альтернативный DNS-сервер: **10.0.2.1**

– натисніть **ОК** => **ОК.**

Закрийте вікно **Центр управления сетями и общим доступом.**

2.3.1 Підключення клієнтського робочого місця до домену

Підключіть комп'ютер з мережевим ім'ям **rmf52** до домену **rmf151.domain01.local,** тобто до домену, в якому контролером домену є комп'ютер з фізичним ім'ям **RMF01**:

– **Пуск => Компьютер** (правою кнопкою миші) => **Свойства => Дополнительные параметры системы =>** вкладка **Имя компьютера => Изменить;**

– у вікні **Изменение имени компьютера или домена** вибрати вкладку **Имя компьютера**, вибрати опцію **Является членом домена,** в текстовому полі впишіть **domain01.local** (у вас, відповідно, інше ім'я домену) => натисніть **ОК;**

– у вікні **Имя и пароль пользователя в домене** в полі **Пользователь** введіть **Администратор**, а в полі **Пароль – 1q2w3e4r&** або **1q2w3e4r5t&** (для **&** натисніть комбінацію клавіш **Shift+7)**. **Перед введенням пароля встановіть російську розкладку клавіатури** => натисніть **ОК**;

– через деякий час відкриється вікно з запрошенням приєднатися до домену **domain01.local** => натисніть **ОК.**

Погодьтеся з пропозицією перезавантажити комп'ютер, натиснувши **ОК** (при цьому ви повертаєтеся у вікно **Свойства системы**) => натисніть **ОК** => **Да.**

Після перезавантаження комп'ютера (під час якого не забудьте перевести курсор на рядок **Microsoft Windows 7**) виконайте вхід в систему (виберіть змінити користувача, інший користувач):

– пользователь – **DOMAIN01\Администратор;**

– пароль – **1q2w3e4r&** або **1q2w3e4r5t&** (для **&** комбінація клавіш **Shift+7)**. **Перед введенням пароля встановіть російську розкладку клавіатури**.

2.3.2 Створення облікового запису користувача на клієнті

Для цього необхідно виконати наступні дії:

– завантажити **Windows 7** та виконати вхід в режимі адміністратора серверу з паролем **1q2w3e4r&** або **1q2w3e4r5t&;**

– виконати: **Пуск** => **Панель управления** => **Изменение типа учетной записи**;

– у вікні **Учетные записи пользователей** в полі **Пользователи этого компьютера** оберіть => **Додати користувача** => **Petrov;**

– у вікні **Добавление нового пользователя**:

Пользователь: **Petrov**

Домен: **DOMAIN01** (у вас, відповідно, інший домен) натиснути **Далее**.

– обрати **Обычный доступ** і натиснути **Готово**.

Після створення нового користувача увійти в систему під його ім'ям. Для цього натиснути **Ctrl+Alt+Del** і змінити користувача. Виконати вхід в систему:

Пользователь **DOMAIN01\Petrov**

Пароль **1q2w3e4r5t& (**англ. раскладка**).**

2.4 Установка UserGate на сервері

Запустити інсталяційний файл програми **User Gate**:

– **Пуск** => **Компьютер** => **MS-DOS (C:)** => папка **Install** => папка **UserGate_v5.2.711** => файл **usergate5_setup**;

– після того, як відкрилось вікно **Программа установки UserGate Proxy & Firewall 5** (рис.2.1), перегляньте інформацію та натисніть => **Далее;**

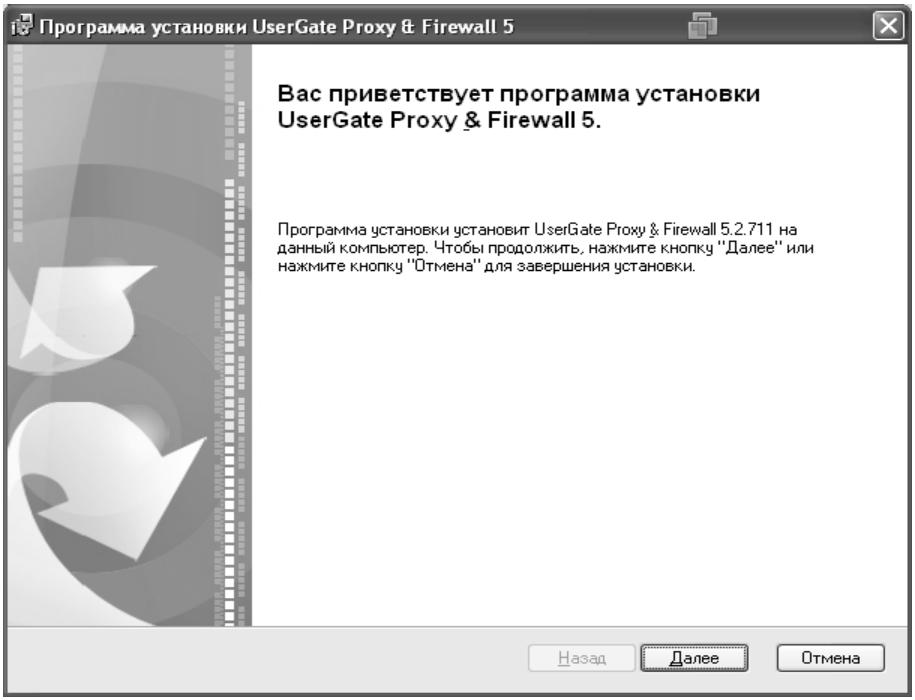

Рисунок 2.1 – Програма установки UserGate Proxy & Firewall 5

– у вікні **Лицензионное соглашение**:

1) ознайомтися з **Лицензионное соглашение**;

2) виберіть пункт **Я принимаю условия лицензионного соглашения**;

3) натисніть **Далее**;

– у вікні **Выборочная установка** (рис.2.2):

1) перегляньте місце встановлення (**Расположение**);

2) у вас має бути**: F:\Program Files\Entensys\UserGate 5\;**

Примітка. UserGate встановлюється на той диск, де встановлена операційна система з якою працюємо**, в нашому випадку диск F:\,** але може бути й інший**;**

3) натисніть кнопку **Далее;**

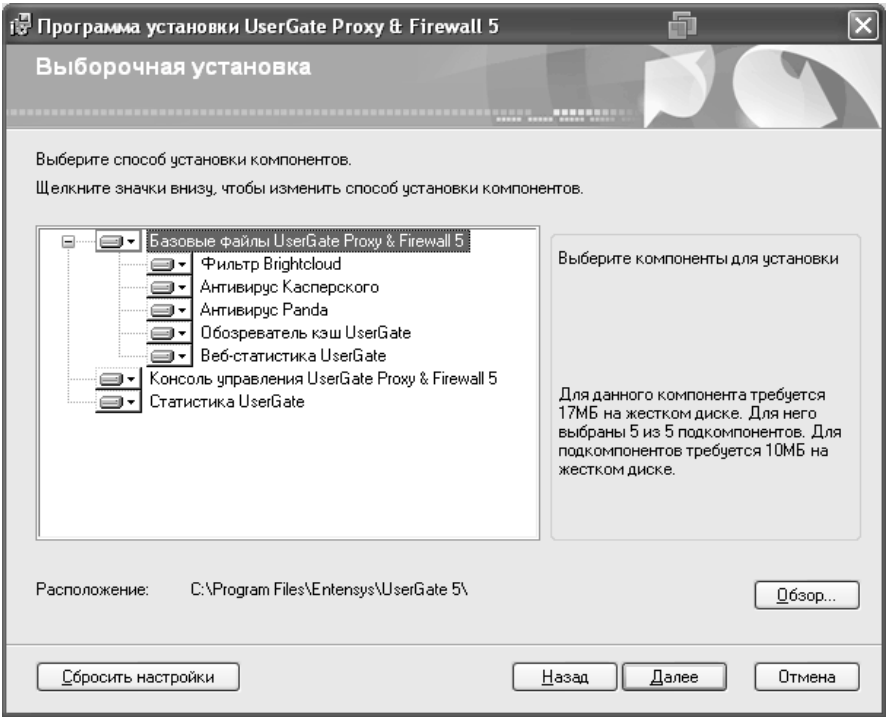

Рисунок 2.2 – Вибіркова установка

– у вікні **Установить UserGate Proxy & Firewall 5**, перегляньте інформацію про можливі дії та натисніть кнопку **Далее**.

Зачекайте поки буде завершено установку **UserGate Proxy & Firewall 5.**

(У процесі установки може вискакувати вікно **Установка оборудования**, (декілька разів) натискаємо клавішу **Все равно продолжить** і програма продовжує в автоматичному режимі встановлюватися на комп'ютер).

При появі вікна **Установка UserGate Proxy & Firewall 5 успешно завершена,** натискаєм кнопку **Готово.**

Погоджуємося на пропозицію перезавантажити комп'ютер, і при подальшому завантаженні не забуваємо перевести курсор на рядок **MS Windows 2008 Server**).

Виконайте вхід до системи:
Пользователь – **Администратор;**
Пароль – **1q2w3e4r&** або **1q2w3e4r5t&** (для **&** натисніть комбінацію клавіш **Shift+7)**.

2.4.1 Налаштування UserGate

Після того, як ви перезавантажили комп'ютер і правильно авторизувалися (ввели правильне ім'я користувача, пароль, зайшли в свій домен) в області трея (там де годинник) з'явиться значок (рис.2.3).

Рисунок 2.3 – UserGate агент

Вам необхідно підвести курсор миші на цей символ і двічі натиснути лівою кнопкою по ньому.

При цьому відкриється вікно **Консоль администратора UserGate 5** (рис.2.4)**,** яка дозволяє виконувати всі наступні дії з адміністрування та використання, наведених вище, функцій програмного забезпечення UserGate.

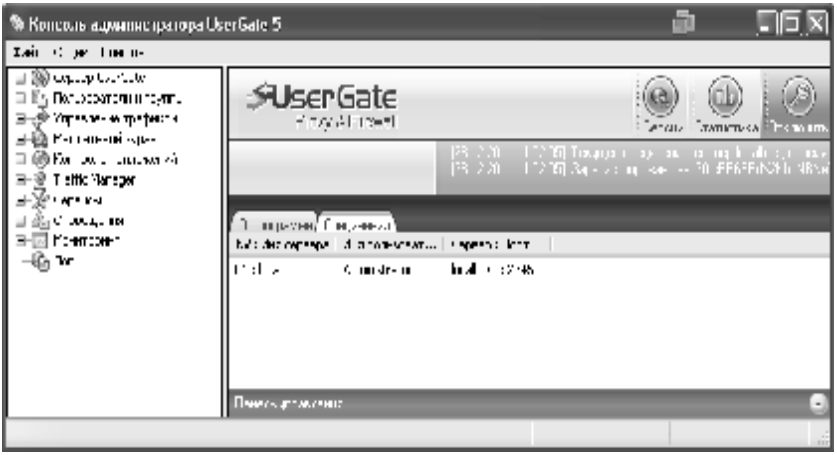

Рисунок 2.4 – Консоль адміністратора UserGate 5

2.4.2 Запуск сервера UserGate

Запускаємо сервер **UserGate,** натисканням подвійного клацання миші на рядок **01:local Administrator localhost: 2345** (або ж клацаємо по значку **UserGate агент**, який знаходиться в треї і вибираємо з контекстного меню **Запустить сервер)**. З'явиться діалогове вікно: "**Информация: Вы запустили консоль администрирования первый раз. Запустить мастер настройки UserGate?**" (рис.2.5).

Примітка. Якщо потрібно зупинити сервер, за допомогою подібного способу, можна зупинити сервер, натиснувши правою кнопкою миші по значку **UserGate агент,** який знаходиться в треї і вибрати з контекстного меню **Остановить сервер**.

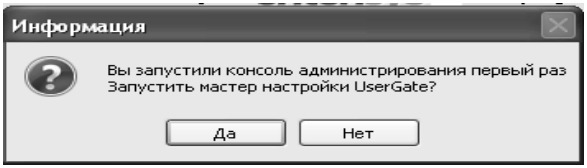

Рисунок 2.5 – Інформація

Не погоджуємося натисканням кнопки **Нет.**

Для зміни типу з'єднання перейдемо у вкладку **Интерфейсы** для цього необхідно натиснути на + **Сервер UserGate** вибрати тип **Интерфейса WAN.**

У вікні **Редактировать интерфейс** в полі **Название** має бути адреса **10.0.9.151 (основна)** (у вас, відповідно, інша адреса), тип інтерфейсу вибрати **WAN.**

Ті ж дії виконати для інтерфейсу **LAN і** вибрати **Тип интерфейса LAN з** адресою **192.168.0.151** (у вас, відповідно, інша адреса).

Натисніть кнопку **Да** на рядку **Сохранить изменения**.

2.4.3 Додавання групи та користувача

Для створення нової групи:

– перейти у вкладку **Группы**;

– створити **Группу**:

1) у вікні **Группы**, натисніть кнопку **Добавить**;
2) у рядку **Название группы** вписати **Группа1**;
3) натисніть кнопку **ОК** => **Сохранить изменения**.

Після створення **Группы** перейти у вкладку **Пользователи и Группы** => **Пользователи**, необхідно створити користувача.

Для цього:

– натисніть на кнопку **Добавить**, яка знаходиться знизу вікна програми;

– з'являється вікно **Добавление пользователя. Основная информация** (рис.2.6);

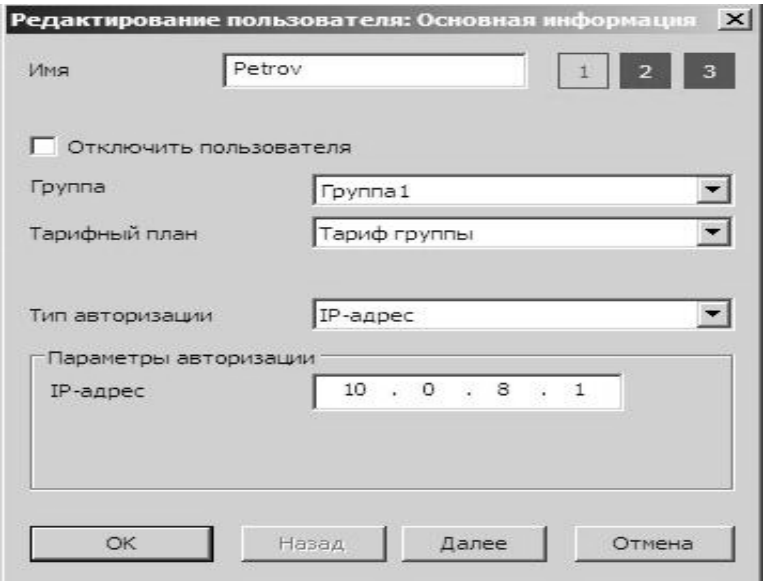

Рисунок 2.6 – Редагування користувача: основна інформація

– у цьому вікні:

1) в рядку **Имя** вписуємо ім'я **Petrov** (у вас. відповідно інше, ім'я);
2) в пункті **Группа** вибиріть **Группа1**;
3) **Тарифный план** також залишаємо в початковому значенні;
4) **Тип авторизации - IP-адрес;**
5) **Параметры авторизации:**

IP-адрес **192.168.0.52 (клиент Win7)**

– натисніть **ОК** => **Сохранить изменения.**

2.4.4 Додавання та видалення правил

Перейти у вкладку **Управление трафиком**, вибрати **Правила:**

– у вікні **Правила** натиснітьь кнопку **Добавить**;
– у вікні **Основное** у рядку **Имя правила** ввести **Правило 1**:

1) **Тип логики** вибрати **ИЛИ;**
2) в **Объект** вибрати **Соединение;**
3) в пункті **Действие** вибрати **Закрыть;**
4) натисніть кнопку **Далее**;

– у вікні **Протоколы** вибрати протокол **HTTP** і натисніть кнопку **Далее;**

– у вікні **Время и праздники** вибрати **Все** (це означає, що це правило буде застосовуватися до всіх днів поточного місяця) і натисніть кнопку **Далее;**

– у вікні **Лимиты** переглянути інформацію і натиснути кнопку **Далее;**

– у вікні **Фильтры** вибрати **URL-адреса;**

– у графі **Список адресов** на порожньому білому полі натисніть правою кнопкою миші і з контекстного меню виберіть **Добавить**;

– у вікні, яке з'явилось, виберіть пункт **Добавить в список URL** і в рядку впишіть **google.com**;

– натисніть кнопку **Добавить и закрыть** (рис.2.7).

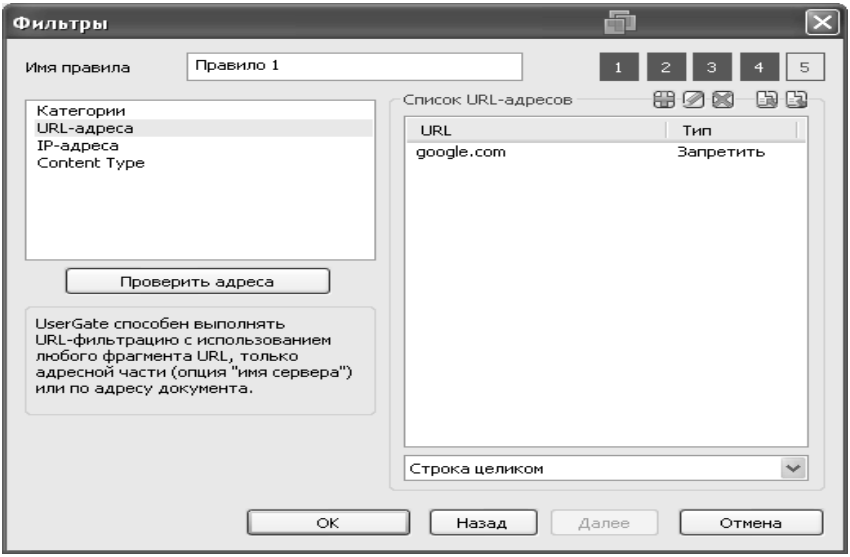

Рисунок 2.7 – Фільтри

Застосування Правила 1:

– у вікні **Консоль администратора UserGate5**:

1) розкрити вкладку **Пользователи и группы**;

2) вибрати **Группы** у правому вікні натиснути правою кнопкою миші **Группа 1**;

3) в контекстному меню вибрати **Редактировать группу**;

– у вікні **Группа 1**:

1) в полі **Выбирете правило для группы** відмітити **Правило 1**;

2) натисніть **ОК**;

3) зберегти зміни, натиснувши **Да**;

– на **клієнтській машині** перевірити роботу **Правила 1**, запустивши Інтеренет.

Додавання нового Правила 2. Перевірка роботи HTTP протокола:

– у вікні **Консоль администратора UserGate5** розкрити вкладку **Управление трафиком => правила =>Добавить;**

– у вікні **Основное** вибрати **Имя правила => Правило 2.**

Тип логики => ИЛИ, натисніть **Далее.**

– у вікні **Протоколы** відмітити галочкою всі протоколи, натисніть **Далее**;

– у вікні **Время и праздники** натисніть **Все**, натисніть **ОК**. Зберегти всі налаштування, натиснувши **Да**;

– застосувати правило для **Группы**. Перевірити роботу **Правила 2** на RMF2.

2.4.5 Тестування роботи UserGate в режимі користувача

Відкрийте вікно браузера:

– **Пуск => Internet Explorer => Остановить;**

– **Сервис => Свойства обозревателя => Подключения => Настройка сети;**

– у вікні **Настройка параметров локальной сети** в полі **Использовать прокси-сервер для локальных подключений** встановіть:

Адрес: 192.168.0.151 (адреса внутрішнього адаптеру серверу**)**

Порт 8080

– встановіть галочку **Не использовать прокси-сервер для локальных адресов;**

– натисніть **ОК =>ОК,** закрийте вікно браузера.

Запустіть Інтернет. При першому запуску система запросить ввести пароль при вході.

Примітка. Пароль на вхід до мережі Інтернет студенти повинні отримати в ауд.148 (можна використати пароль іншого студента групи).

2.4.6 Каскадні проксі

Для **створення каскадного проксі** виконайте наступні дії:

– вибиріть **Сервисы** => перейти за посиланням **Каскадные прокси**;

– у вікні, яке з'явилось, на білій області натиснути правою кнопкою миші та в контекстному меню вибрати **Добавить прокси**;

– у вікні **Добавить новый прокси сервер**:

1) у рядку **Название** ввести **Proxy**;

2) у рядку **Введите IP адрес и порт прокси** ввести **10.0.2.1 Порт 8080, Тип прокси – http**;

– ставимо галочку на **Авторизация** і вводимо:

Имя пользователя **Petrov** (у вас, відповідно, "своє" ім'я)

Пароль (пароль для входу в Інтернет)

– натисніть **ОК;**

Зберігти дані, натиснувши **Да.**

Для **налаштування проксі** виконайте наступні дії**:**

– вибиріть **Сервисы** => **Настройка прокси**;

– вибрати **Протокол HTTP;**

– у вікні **Настройка HTTP-прокси** поставити галочку **Включить HTTP-прокси**;

– вибрати інтерфейс **192.168.0.151** (у вас, відповідно, інша адреса);

– **Каскадный прокси** вибрати **Proxy**;
– натисніть **ОК.**

Зберегти змінення, натиснувши **Да.**

2.5 Підключення до Інтернету

Відкрийте вікно браузера:

– **Пуск => Internet Explorer => Остановить;**

– **Сервис => Свойства обозревателя =>** на вкладці **Общие** у розділі **Домашняя страница** натисніть **пустая =>** перейдіть на вкладку **Подключения => Настройка сети;**

– встановіть галочку **Использовать прокси-сервер для локальных подключений;**

– в полі **Адрес** укажіть **192.168.0.1 (**у вас, відповідно. інша адреса**);**

– в полі **Порт** укажіть **8080;**

- встановіть галочку **Не использовать прокси-сервер для локальных адресов;**

– **ОК => ОК;**

– закрийте вікно браузера.

Контроль виконання завдання:

– на панелі задач в меню **Пуск** вибрати **Internet Explorer** і в адресний рядок браузера задати **URL google.com;**

– **Internet Explorer** виведе повідомлення, що **не может отобразить эту веб-страницу** (значить всі налаштування були зроблені правильно) (рис.2.8).

Рисунок 2.8 – Результати роботи

Після цього переходимо до налаштування **Каскадных прокси**, для цього:

– натисніть на посилання **Главного меню** програми **Каскадные прокси**, після цього виберіть **HTTP** (ставимо галочку);

– у вікні **Настройка HTTP-прокси** виберіть:

Интерфейсы **192.168.0.151**
Порт **8080**

– натисніть кнопку **ОК**.

2.6 Відновлення комп'ютерів в початковий стан

(підлягає обов'язковому виконанню)

На **RMF2** видалити користувача **Petrov**, вивести машину **RMF2** з домену **domain01.local** і ввести в робочу групу **WORKGROUP.** Перевірити налаштування нижнього мережевого адаптера:

IP-адрес: **10.0.9.52** (у вас, відповідно, інша адреса мережевого адаптера)
Маска подсети: **255.255.255.0**
Основной шлюз: **10.0.9.100**

Предпочитаемый DNS-сервер: **10.0.2.1**

Відновити налаштування верхнього мережевого адаптера, тобто зробити налаштування в автоматичному режимі.

На **RMF1**:

– видалити програму **UserGate5**;

– видалити створений обліковий запис користувача **Petrov** і групу **gr_petrov;**

– перевірити налаштування нижнього мережевого адаптера:

IP-адрес: **10.0.9.151** (адреса адаптера вашого серверу)

Маска подсети: **255.255.255.0**

Основной шлюз: **10.0.9.100**

Предпочитаемый DNS-сервер: **10.0.2.1**

– відновити налаштування верхнього мережевого адаптера, тобто зробити налаштування в автоматичному режимі.

– відновити налаштування Інтернету.

2.7 Зміст письмового звіту

1. Теоретичні відомості.
2. Загальні схеми.
3. Хід роботи.
4. Відповіді на контрольні питання.

2.8 Контрольні питання

1. UserGate. Призначення і принцип роботи.
2. Основні функції UserGate?
3. Як налаштувати доступ в Інтернет і за допомогою яких засобів здійснюється інформаційна безпека?
4. Які засоби використовуються для адміністрування мережі?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Моримото Р. Microsoft Windows Server 2008 R2. Полное рук-во / Моримото Р., Ноэл М., Драуби О., Мистри Р., Амарис К. // Пер. с англ. — М. : ООО "И.Д. Вильямс", 2011. — 1456с. : ил.

2. Нортроп Т. Проектирование сетевой инфраструктуры Windows Server 2008. Учебный курс Microsoft / Т. Нортроп, Дж.К.Макин // Пер. с англ. — М. : Издательство «Русская Редакция», 2009. — 592с. : ил.

3. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. — 4-е изд. — СПб.: Питер, 2011. — 944с.: ил.

4. Одом, Уэнделл. Официальное руководство по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 / Уэнделл Одом. – 2-е изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2010. – 672 с. – ISBN 978-5-8459-1439-2.

5. Одом, Уэнделл. Официальное руководство по подготовке к сертификационным экзаменам CCNA ICND2 / Уэнделл Одом. – 2-е изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2012. – 736 с. – ISBN 978-5-8459-1442-2.

6. Ватаманюк А.И. Создание и обслуживание сетей в Windows 7 / А.И.Ватаманюк. – СПб.: Питер, 2010. – 224 с.: ил. – ISBN 978-5-49807-499-3.

7. Бакланов И.Г. NGN: принципы построения и организации / И.Г. Бакланов, под ред. Ю.Н. Чернышова. – М.: Эко-Трендз, 2008. – 400 с. – ISBN 978-5-88405-083-9.