Lucrarea de laborator nr. 5

Protecția comunicațiilor: Firewall și VPN

Scop

Scopul lucrării este configurarea și analiza mecanismelor de protecție a comunicațiilor de rețea prin utilizarea firewall-urilor și a unei conexiuni VPN, precum și compararea traficului de rețea protejat și neprotejat.

Cerință generală

Configurați o rețea care să includă **cel puțin două firewall-uri** și o **conexiune VPN în modul transport**. Analizați diferențele dintre traficul de rețea transmis în mod neprotejat și traficul transmis prin VPN.

Cerințe obligatorii

1. Descrierea topologiei de rețea

Descrieți topologia rețelei utilizate, indicând:

- numărul de sisteme implicate;
- poziționarea firewall-urilor;
- rolul fiecărui sistem (client, gateway, punct de acces).

Topologia poate fi realizată fizic sau virtual (mașini virtuale).

2. Configurarea firewall-urilor

Configurați **două firewall-uri** (software sau hardware), indicând:

- tipul firewall-ului utilizat;
- regulile de filtrare aplicate;
- politica implicită (permitere / blocare).

Documentați diferențele de configurare dintre cele două firewall-uri.

3. Testarea regulilor firewall

Testați și documentați:

- traficul permis;
- traficul blocat;
- comportamentul sistemului la încercări de acces neautorizat.

4. Configurarea conexiunii VPN

Configurați o conexiune **VPN în modul transport**, indicând:

- tipul VPN-ului utilizat;
- algoritmii de criptare și autentificare;
- parametrii principali de configurare.

5. Capturarea traficului de rețea

Realizați capturi de trafic pentru:

- comunicații neprotejate;
- comunicații protejate prin VPN.

Capturile trebuie realizate folosind un instrument de analiză a traficului (de exemplu, Wireshark).

6. Analiza comparativă a traficului

Analizați și comparați:

- vizibilitatea informațiilor în traficul neprotejat;
- nivelul de confidențialitate al traficului protejat;
- diferențele observate la nivel de protocoale și conținut.

Лабораторная работа №5

Защита коммуникаций: Firewall и VPN

Цель работы

Целью данной лабораторной работы является настройка и анализ механизмов защиты сетевых коммуникаций с использованием **межсетевых экранов (firewall)** и **VPN-соединения**, а также сравнение защищённого и незащищённого сетевого трафика.

Общее требование

Настройте сеть, включающую **как минимум два межсетевых экрана** и **VPN-соединение в транспортном режиме**. Проанализируйте различия между сетевым трафиком, передаваемым в незащищённом виде, и трафиком, передаваемым через VPN.

Обязательные требования

1. Описание сетевой топологии

Опишите используемую сетевую топологию, указав:

- количество задействованных систем;
- расположение межсетевых экранов;
- роль каждой системы (клиент, шлюз, точка доступа).

Топология может быть реализована как **физически**, так и **виртуально** (с использованием виртуальных машин).

2. Настройка межсетевых экранов (Firewall)

Настройте **два межсетевых экрана** (программных или аппаратных), указав:

- тип используемого firewall;
- применяемые правила фильтрации;
- политику по умолчанию (разрешающая / запрещающая).

Задокументируйте различия в конфигурации между двумя firewall-ами.

3. Тестирование правил firewall

Проведите тестирование и задокументируйте:

- разрешённый трафик;
- заблокированный трафик;
- поведение системы при попытках несанкционированного доступа.

4. Настройка VPN-соединения

Настройте **VPN-соединение в транспортном режиме**, указав:

- тип используемого VPN;
- алгоритмы шифрования и аутентификации;
- основные параметры конфигурации.

5. Захват сетевого трафика

Выполните захват сетевого трафика для:

- незащищённых коммуникаций;
- коммуникаций, защищённых с помощью VPN.

Захват трафика должен быть выполнен с использованием инструмента анализа сетевого трафика (например, **Wireshark**).

6. Сравнительный анализ трафика

Проанализируйте и сравните:

- степень видимости информации в незащищённом трафике;
- уровень конфиденциальности защищённого трафика;
- различия, наблюдаемые на уровне протоколов и содержимого.