Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії
Кафедра Захисту інформації

Методичні матеріали для виконання лабораторних робіт

з дисципліни “Захист інформації в інформаційно-комунікаційних системах”
частина 2

Вінниця

ЗМІСТ

Лабораторна робота № 1 Мережеві налаштування мережевих адаптерів віртуальної машини

Мета роботи: навчитися налаштовувати мережеві адаптери для зв'язку між віртуальними машинами.

Хід роботи

1. Встановити віртуальну машину з операційною системою CentOS 6.
2. В налаштуваннях мережевих адаптерів віртуальної машини встановити тип підключення **«сетевой мост».**
3. Знайти зареєстровані в системі мережеві адаптери командою:

   ifconfig –a
4. У файлі

   /etc/sysconfig/network-scripts/ifcfg-eth2

   сконфігурувати порт (MAC ,IP-адреси) редагуючи відповідний файл (за допомогою команди vi)

   vi /etc/sysconfig/network-scripts/ifcfg-eth2
5. Перезавантажити служби мережі командою:

   service network restart
6. Повторити п. 1-5 для другої віртуальної машини,.
7. Перевірити зв'язок у обидві сторони за допомогою команди ping.
8. Виконати звіт з лабораторної роботи, який включає в себе скріншоти виконаних команд.

Контрольні питання

1. Які типи підключення використовуються?
2. Що таке IP-адреса?
3. Які особливості конфігурування портів, які параметри є обов'язковими?
4. Що таке «ping»? Який протокол використовується?
5. Які параметри можна вказати у ping?
6. Які параметри відображаються за командою ping?
7. Як визначити затримки у мережі?
8. Як визначити чи всі пакети дійшли?
9. Як визначити скільки маршрутизаторів пройшов пакет?
10. Як визначити чи правильна послідовність пакетів?

Лабораторна робота №2. Налаштування Basic HTTP-автентифікаії

Мета: отримати практичні навички встановлення та налаштування веб-серверу та організації авторизованого доступу до нього засобами операційної системи CentOS

Хід роботи

1. Завантажити віртуальну машину із ОС CentOS.
2. Налаштувати мережеве з'єднання із можливістю досту до мережі Інтернет (див. лаб. роб. 1).
3. Встановити та налаштувати веб-сервер Nginx

3.1 Додавання в репозиторій

3.2 Установка Nginx

- встановити веб-сервер nginx за допомогою yum :

yum install nginx

- додайте nginx в автозавантаження :

chkconfig nginx on

3.3 Базовая настройка Nginx

- зробіть резервну копію конфігураційних файлів:

cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.back

cp /etc/nginx/conf.d/default.conf /etc/nginx/conf.d/default.conf.back

- відкрийте файл конфігурації nginx /etc/nginx/nginx.conf та змініть значення параметру worker_processes. Воні повинні дорівнювати кількості процесорів на сервері.

worker_processes 1;

- для з'ясування кількості процесів команда :

lscpu | grep '^CPU(s)'

- збережіть та закрийте файл.
- відредагуйте файл /etc/nginx/conf.d/default.conf. Задайте ім'я сервера:

server_name example.com;

- збережіть та закрийте файл.

3.4 Запустіть ngnix :

service nginx start

Перевірте правильність налаштування та працездатність веб-серверу увівши в адресному рядку браузера ім'я сервера.

4. Налаштування Basic HTTP-авторизації

4.1 Відредагуйте конфігураційний файл (default.conf) веб-серверу у розділі location {…}. Замініть

```
location / {
root   html;
index  index.html index.htm;
}
```

на наступне:

```
 location / {
 auth_basic            "closed site";
 auth_basic_user_file  htpasswd;
```

```
root   html;
index  index.html index.htm;
}
```

4.2 Перевантажити сервер. Після цього при відкритті сайту з’являється вікно з автентифікацією.

4.3 Створити файл з логіками та паролями користувачів, що мають доступ до сервера.

Файл паролів у папці etc/nginx/htpasswd. Формат:

коментар
імя1:пароль1
імя2:пароль2: коментар
імя3:пароль3

Паролі генеруються за допомогою утіліти crypt у htpasswd. Команда.

sudo htpasswd –c –b -d htpasswd nrg 12345

"-d" – вибір криптофункції "crypt"
"-b" – вказати ім’я файлу
"-c" – створити новий файл
htpasswd -- ім’я нового файлу
nrg -- ім’я користувача, що додається
12345 -- пароль користувача

4.4 Створіть декілька логінів та паролей, до одного з яких додайте коментар. Відобразіть вміст файлу.

4.5 Перевантажити сервер.

4.6 Після цього при відкритті сайту з’являється вікно з автентифікацією.

4.7 Введіть правильні та неправильні автентифікаційні дані, для перевірки налаштувань.

Завдання

1. Відтворити усі описані дії по встановленню та налаштуванню авторизації до http-серверу.
2. Організувати парольний доступ до декількох папок на сервері попередньо їх створивши.
3. Організувати обмеження доступу до сервера по певній ip-адресі, наприклад сусіднього ПК у комп’ютерній лабораторії та перевірити працездатність налаштувань.
4. *Організувати можливість авторизації клієнта до сервера , який базується на результаті під запиту (http://nginx.org/ru/docs/http/ngx_http_auth_request_module.html).
5. **Організувати можливість авторизації клієнта до сервера , який базується на JWT.
6. Оформити звіт по виконаним завданням із відповідними екранними формами та коментарями до них.
7. Зробити ґрунтовні висновки по роботі

Контрольні запитання

1. Поняття авторизації веб-сервера
2. Опишіть процес встановлення та налаштування веб серверу під CentOS
3. Що таке Basic HTTP-автентифікація?
4. Які інші види автентифікації на веб-сервері Ви знаєте?
5. Опишіть структуру конфігураційного файлу веб-сервера?
6. Опишіть процедуру встановлення обмеження доступу до сервера?
7. Чим базова автентифікація apache відрізняється від базової автентифікації nginx?

Лабораторна робота №3 Налаштування віртуальних локальних мереж ч.1

Мета роботи: навчитися налаштовувати мережеві комутатори для створення віртуальних локальних мереж VLAN.

Хід роботи

1. Нехай є мережа як показано на рис.1. Необхідно сегментувати відділи A та B. В тому числі обмежити і широкомовний трафік. Номери VLAN обирати відповідно до варіанту.

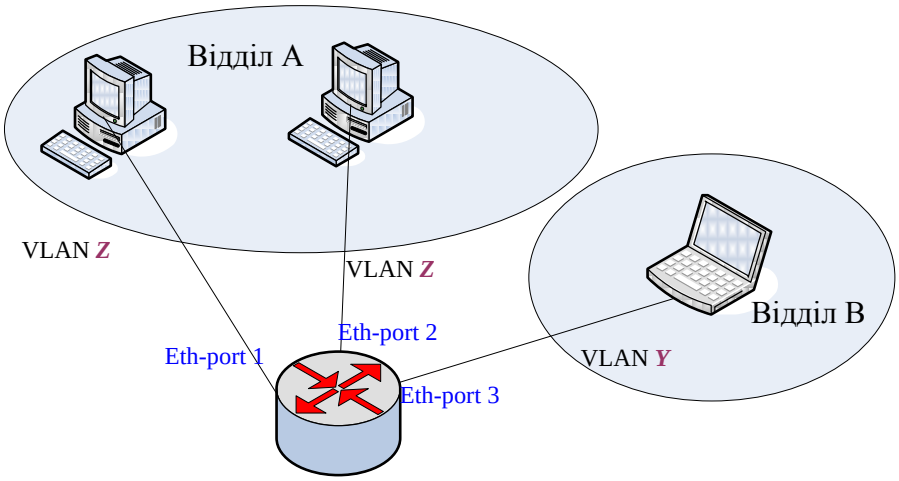

Рисунок 1 – Схема мережі

2. Призначити IP-адреси в мережах виходячи з діапазону 192.168.Z.0/24 для мережі A та 192.168.Y.0/24 для мережі B.
3. Створити інтерфейс vlan, пов’язавши його з lan-інтерфейсом та вказати VLAN ID.
4. Вказати номер порту комутатора, на якому сконфігуронвана дана vlan.
5. Перевірити налаштування використовуючи команду ping.
6. Сконфігурувати vlan для схеми з курсового проекту.
7. Змоделювати у Packet Tracer та GNS 3
8. Виконати звіт з лабораторної роботи, який включає в себе скріншоти виконаних команд.

Контрольні питання

1. Чим відрізняються фізична та логічна сегментація мережі?
2. Опишіть поняття віртуальної локальної мережі (VLAN)?
3. В чому суть VLAN на основі портів (Port-based VLAN)?
4. Як налаштувати VLAN на основі портів (Port-based VLAN) у Packet Tracer?

Лабораторна робота №4 Налаштування віртуальних локальних мереж 802.1q

Мета роботи: навчитися налаштовувати мережеві комутатори для створення віртуальних локальних мереж VLAN за протоколом 802.1q

Хід роботи

1. Обираємо мережу з визначеними IP адресами.
2. Налаштовуємо vlan за стандартом 802.1q.
3. Обрати один комп'ютер з одного відділу і зв'язати з комп'ютером з іншого відділу. Щоб це зробити треба в налаштуваннях комутатора до відповідного інтерфейсу обрати щойно створений vlan.
4. Змінити режим роботи маршрутизатора з Access у Trunk. Це робиться для передачі трафіку декількох vlan. Це є обов'язковою опцією, якщо в мережі використовується декілька комутаторів.

У Cisco Packet Tracer 6.2 за замовчуванням активовано стандарт 802.1q.

У інших версіях потрібно в консолі комутатора ввести:

Switch#conf t (перейти у режим налаштування)

Switch(config)#interface FastEthernet0/1 (вибираємо потрібний і-фейс)

Switch(config-if)# switchport trunk encapsulation dot1q (активація 802.1q)

Switch(config-if)# switchport mode trunk (перехід комутатора у режим trunk)

Switch(config-if)# switchport trunk allowed vlan 3,4 (які vlan будуть працювати у режимі trunk)

Switch(config-if)# no shut (активація і-фейсу)

Також, можлива активація протоколу ISL, для цього потрібно замінити dot1q на:

Switch(config-if)# switchport trunk encapsulation isl

Перевіряємо:

Switch#show int trunk

5. Налаштувати

```
R1(config)# interface fa0/0.2
R1(config-subif)# encapsulation dot1q 2
R1(config-subif)# ip address 10.0.2.1 255.255.255.0
```

Контрольні питання

1. Обгрунтуйте необхідність використання VLAN на основі стандарту IEEE 802.1Q
2. Які особливості VLAN на основі стандарту IEEE 802.1Q?
3. Наведіть формат кадру 802.1Q.
4. Наведіть правила руху кадрів у комутаторі.
5. Наведіть правила вхідного трафіку.

6. Наведіть правила руху між портами.
7. Наведіть правила вихідного трафіку.
8. Поясніть поняття статичних та динамічних VLAN.

Лабораторна робота № 5 «Налаштування між мережевого екрану»

Мета роботи: навчитися виконувати налаштування між мережевого екрану

Хід роботи

Частина 1. Налаштування міжмережевого екрану CentOS 6

1. В ЛР 1 було налаштовано дві віртуальні машини та встановлено мережевий зв'язок між ними.
2. Перевірити зв'язок між двома віртуальними машинами за допомогою команди ping.
3. Перевірити поточні налаштування між мережевого екрану iptables, за допомогою команди:

```
iptables –L
```

4. Видалити стандартно встановлені правила за допомогою команди

```
iptables –F
```

і бачимо, що усі правила очищено.

5. Заборонити на першій віртуальній машині виконання команди ping, для чого за допомогою інтерфейсу керування роботою міжмережевого екрану, налаштувати правило в iptables на заборону передачі ICMP пакетів.

```
iptables -I INPUT -p icmp --icmp-type 8 –j DROP
```

6. Перевірити, що правило встановлено у ланцюгу iptables:
7. Перевіряємо правильність встановленого правила, за допомогою команди ping, що у результаті показує як пакети блокуються у заданому нами напрямку.
8. Перевірити чи залишились інші види доступу, наприклад через SSH.
9. Виконати налаштування прав міжмережевого екрану відповідно до заданого варіанту.

Таблиця 5.1

Вариант	Завдання
1	− Заборонити/дозволити вхідний трафік конкретній ip-адресі, наприклад основна машина або інша віртуальна або навіть глобальна − заборонити вхідний трафік по протоколу telnet (локально) − заборонити вихідний трафік по протоколу telnet до конкретної ip-адреси
2	Заборонити/дозволити вихідний трафік до конкретної ip-адреси, наприклад основна машина або інша віртуальна або навіть глобальна − заборонити вихідний трафік по протоколу telnet − заборонити вхідний трафік по протоколу telnet конкретній ip-адресі (локально)
3	− Заборонити/дозволити вхідний icmp-трафік конкретній ip-адресі − заборонити вхідний трафік по протоколу ftp (локально) − заборонити вихідний трафік по протоколу ftp до конкретної ip-адреси

4	− Заборонити/дозволити вихідний icmp-трафік до конкретної ip-адреси − заборонити вихідний трафік по протоколу ftp − заборонити вхідний трафік по протоколу ftp конкретній ip-адресі (локально)
5	− Заборонити/дозволити вхідний трафік з конкретної веб-адреси (доменного імені) − заборонити вхідний трафік по протоколу smtp (локально) − заборонити вихідний трафік по протоколу smtp до конкретної адреси-сервера (веб або ip-адреси)
6	Заборонити/дозволити вихідний трафік до конкретної веб-адреси (доменного імені) − заборонити вихідний трафік по протоколу smtp − заборонити вхідний трафік по протоколу smtp конкретній ip-адресі (локально)
7	− Заборонити/дозволити вхідний трафік з конкретної веб-адреси (доменного імені) − заборонити вхідний трафік по протоколу pop3 (локально) − заборонити вихідний трафік по протоколу pop3до конкретної адреси-сервера (веб або ip-адреси)
8	Заборонити/дозволити вихідний трафік до конкретної веб-адреси (доменного імені) − заборонити вихідний трафік по протоколу pop3 − заборонити вхідний трафік по протоколу pop3 конкретній ip-адресі (локально)
9	− Заборонити/дозволити вхідний трафік з конкретної веб-адреси (доменного імені) − заборонити вхідний трафік по протоколу imap (локально) − заборонити вихідний трафік по протоколу imap до конкретної адреси-сервера (веб або ip-адреси)
10	Заборонити/дозволити вихідний трафік до конкретної веб-адреси (доменного імені) − заборонити вихідний трафік по протоколу imap − заборонити вхідний трафік по протоколу imap конкретній ip-адресі (локально)
11	− Заборонити/дозволити вхідний трафік конкретній ip-адресі, наприклад основна машина або інша віртуальна або навіть глобальна − заборонити вхідний трафік по протоколу http (локальний або глобальний) − заборонити вихідний трафік по протоколу http до конкретної ip-адреси
12	Заборонити/дозволити вихідний трафік до конкретної ip-адреси, наприклад основна машина або інша віртуальна або навіть глобальна − заборонити вихідний трафік по протоколу http − заборонити вхідний трафік по протоколу http конкретній ip-адресі (локально)
13	Заборонити/дозволити вихідний трафік до конкретної веб-адреси

	(доменного імені) − заборонити вихідний трафік по протоколу https − заборонити вхідний трафік по протоколу https конкретній ip-адресі (локально)
14	− Заборонити/дозволити вхідний трафік з конкретної веб-адреси (доменного імені) − заборонити вхідний трафік по протоколу https − заборонити вихідний трафік по протоколу https до конкретної адреси-сервера (веб або ip-адреси)
15	− Заборонити/дозволити вхідний трафік конкретній ip-адресі − заборонити вхідний трафік по протоколу dns − заборонити вихідний трафік по протоколу dns до конкретної ip-адреси
16	− Заборонити/дозволити вихідний трафік до конкретної ip-адреси − заборонити вихідний трафік по протоколу dns − заборонити вхідний трафік по протоколу dns конкретній ip-адресі

Частина 2. Налаштування міжмережевого екрану Windows 7

1. Відкрити **Брандмауэр Windows в режиме повышенной безопасности**. Вибрати вузол **Правила для входящих подключений** і вибрати пункт **Новое правило**.
2. Вибрати значення перемикача **Настраиваемые** і перейти далі .
3. Вибрати значення перемикача **Все программы** і перейти далі.
4. Вибрати **Тип протокола**: **ICMPv4**
5. Натиснути кнопку **Настроить** для пункту **Параметры протокола ICMP**
6. Встановити перемикач в **Определенные типы ICMP**, відмітити прапорець **Эхо-запрос**, натиснути **ОК** і перейти далі.
7. На наступному етапі залишити параметри за замовчуванням або якщо необхідно, то обрати необхідні IP-адреси.
8. Вибрати **Разрешить подключение** і перейти далі.
9. Вибрати необхідний профіль, в якому буде використане правило, і перейти далі.
10. Ввести **имя** і **описание**. Натиснути кнопку **Готово**.
11. Перевірити виконання проведених дій та встановлених умов виконавши команду ping в обидві сторони:
12. Виконати налаштування прав міжмережевого екрану відповідно до заданого варіанту.

Частина 3. Налаштування мережевого екрану, скрипти APF

1. Встановити APF . (APF – використовує фільтри на основі iptables, має більш розгалужену і гнучку систему налаштування) на віртуальну машину CentOS, використовуючи такі команди.

```
wget http://www.rfxn.com/downoads/apf-current.tar.gz
tar –zxvf  apf-current.tar.gz
cd apf-9.7-1
```

sh ./install.sh

2. Налаштувати конфігураційний файл за допомогою команди :

vi /etc/apf/conf.apf

3. Для початку встановити мережевий інтерфейс.

DEVEL_MODE= може приймати значення 1 і 0. Значення 0 встановлює режим роботи APF у тестувальному режимі, тобто працює 5 хвилин і потім вимикається. Значення 1 – працює повноцінно.

4. Відедагувати файл

deny/allow_hosts.rules

Для того, щоб дозволяти/блокувати порти (TCP/UDP), прописати IP, які дозволяємо або блокуємо.

5. У файлі

postroute.rules -

прописати правила пакетного фільтра, на основі iptables.

6. Для запуску APF виконати команду:

/usr/local/sbin/apf –(параметр).

Параметри можна передавати :

-s - запуск

-r - рестарт

-f - стоп

-l - статистика

-st- статус

7. Скористатися командою

service apf (restart,start,stop).

8. Перевірити мережеві налаштування адаптера

vi /etc/sysconfig/network-scripts/ifcfg-eth0

9. Перезавантажити мережевий сервіс:

service network restart

10. Перезавантажити сервіс

apf: service apf restart

11. Переглядаємо правила iptables, які прописав сервіс apf, та записуємо ці правила у файл:

iptables –L > /rules_iptables.apf,

переглядаємо отриманий файл

Виконати звіт з виконаних робіт, в тому числі показати скріншоти та проаналізувати правила, які встановлює Apf

Частина 4 (опційна)

Дослідити програмне забезпечення, що виконує функції міжмережевих екранів для мобільних платформ. Продемонструвати приклади їх застосування

Лабораторна робота №6 Дослідження протоколу SSL. Налаштування підтримки захищених HTTP- з'єднань (HTTPS)

Мета: дослідити особливості функціонування протоколу SSL та отримати практичны навички по створенню вдасних сертифікатів засобами ОС сімейства Linux.

Хід роботи

Частина 1. Створення SSL-сертифікату для веб-серверу Nginx в ОС CentOS.

1. Паредбачається, що ви уже маєте налаштовану віртуальну машину на основі CentOS із встановленим веб-сервером Nginx з лабораторноъ роботи №2.

2. Створюємо каталог для збереження сертифікатів

```
mkdir /etc/nginx/ssl
```

3. Генеруємо в створений каталог файли сертифікату:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/nginx/ssl/nginx.key -out /etc/nginx/ssl/nginx.crt
```

У ході генерування будуть задані деякі запитання для встановлення службової інформації.

4. Додаємо до файлу конфігурації nginx ще одну секцію server такого виду:

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        listen 443 ssl;

        root /usr/share/nginx/html;
        index index.html index.htm;

        server_name your_domain.com;
        ssl_certificate /etc/nginx/ssl/nginx.crt;
        ssl_certificate_key /etc/nginx/ssl/nginx.key;

        location / {
                try_files $uri $uri/ =404;
        }
}
```

5. Перезапускаємо сервіс:

```
service nginx restart
```

6. Перевірка роботи сервера в захищеному режимі

Частина 2. Захоплення та аналіз пакетів в SSL сесії

Першим кроком є захоплення пакетів в SSL сесії. Щоб зробити це, ви повинні перейти на свій улюблений інтернет-магазин і почати процес покупки товару (але відмінити, перш ніж здійснити покупку!). Після

захоплення пакетів Wireshark , ви повинні встановити фільтр так, щоб він відображав тільки кадри Ethernet, які містять записи SSL відправлені і отримані від хоста. (Запис типу SSL-це те ж саме, що і повідомлення SSL). Ви повинні отримати щось на зразок результату зображеного на рисунку 1.
Якщо у вас є труднощі з перехопленням пакетів, ви можете завантажити архів http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip і розпакувати файл перехоплення пакетів *ssl-ethereal-trace-1.*

2. Огляд перехоплених файлів

Wireshark повинен відображати тільки Ethernet кадри, які мають SSL записи. Важливо мати на увазі, що кадр Ethernet може містити один або декілька записів SSL. (Це дуже відрізняється від HTTP, де кожен кадр містить або одне повне повідомлення HTTP або частину повідомлення HTTP.) Крім того, якщо SSL запис не може повністю вміститися в кадр Ethernet, то він буде пересланий у кількох кадрах.
Дайте відповідь на наступні питання. Коли це можливо покажіть роздруківку пакета за допомогою якої Ви дали відповідь на питання. Підпишіть роздруківку, щоб пояснити свою відповідь. Щоб роздрукувати пакет використайте *File->Print*, оберіть *Selected packet only*, оберіть *Packet summary line*, і оберіть мінімальну кількість деталей пакету які потрібні Вам для відповіді.

Хід виконання

1. Для кожного з перших 8 кадрів Ethernet, вказати джерело кадру (клієнта або сервера), визначити кількість записів SSL, які включені в кадрі, і список типів SSL записів, включених в кадрі. Намалюйте часову діаграму між клієнтом і сервером, з одного стрілкою для кожного запису SSL.
2. Кожен з SSL записів починається з трьох однакових полів (можливо, з різними значеннями). Один з цих полів "тип вмісту" і має довжину один байт. Перерахуйте всі три поля і їх довжини.
1. Розгорнути запис ClientHello. (Якщо ваше перехоплення містить кілька записів ClientHello, розкрити кадр,у якому міститься перший запис ClientHello.) Яке значення типу вмісту?
2. Чи містить запис ClientHello одноразове слово (також відоме як "виклик")? Якщо так, яке значення матиме “виклик” в шістнадцятковій системі числення?
3. Чи запис ClientHello називає які кібер-номери він підтримує? Якщо так, у першому з перерахованих номерів, якими є алгоритм з відкритим ключем, з симетричні ключем, і хешем?
4. Знайдіть запис SSL ServerHello. Чи вказує цей запис на обраний шифр? Які алгоритми використовуються в обраному шифру?
5. Чи має це запис одноразове слово? Якщо так, то якої довжини? Яке призначення клієнтських і серверних одноразових слів у SSL записі?
6. Чи містить цей запис ID сесії? Що є метою ID сесії?
7. Чи містить цей запис сертифікат, чи сертифікат включений в окремий запис. Чи можна вмістити сертифікат в один Ethernet кадр?

8.Знайдіть запис обміну клієнтськими ключами. Чи містить цей запис pre-master secret? Для чого цей секрет використовується? Чи є секрет зашифрованим, якщо так, то яким чином? Яку довжину має зашифрований секрет?

9. Яка ціль запису Change Cipher Spec? Скільки байт у записі, що ви перехопили ?

10. Що шифрується у зашифрованому записі-рукостисканні, і яким чином?

11. Чи сервер також відправляє запис зміни шифру і зашифрований запис-рукостискання для клієнта? Як ці записи відрізняються від тих, що відправлені клієнтом?

12. Як програмні дані шифрується? Чи записи, що містять дані програми включають MAC? Чи може Wireshark розрізнити зашифровані дані додатку і MAC?

13. Прокоментувати і пояснити все те, що ви знайшли цікавим у перехоплених даних.

Контрольні питання

1. Протокол SSL/TLS (VPN на транспортному рівні)
2. Протокол SSL/TLS. Архітектура
3. Протокол SSL/TLS. *Change Cipher Spec Protocol*
4. Протокол SSL/TLS. *Alert Protocol*
5. Протокол SSL/TLS. Handshake protocol
6. Протокол SSL/TLS. *SSL Record Protocol*
7. Протокол SSL/TLS. Сесії
8. Протокол SSL/TLS. Переваги та недоліки