

УО «Гомельский государственный университет им. Ф. Скорины»  
Физический факультет  
Кафедра общей физики

## *ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1*

### Основы администрирования межсетевого экрана D-Link DFL-860

Проверил:  
Грищенко В.В.

Выполнили:  
студент группы МС-42  
Гончаров Владислав

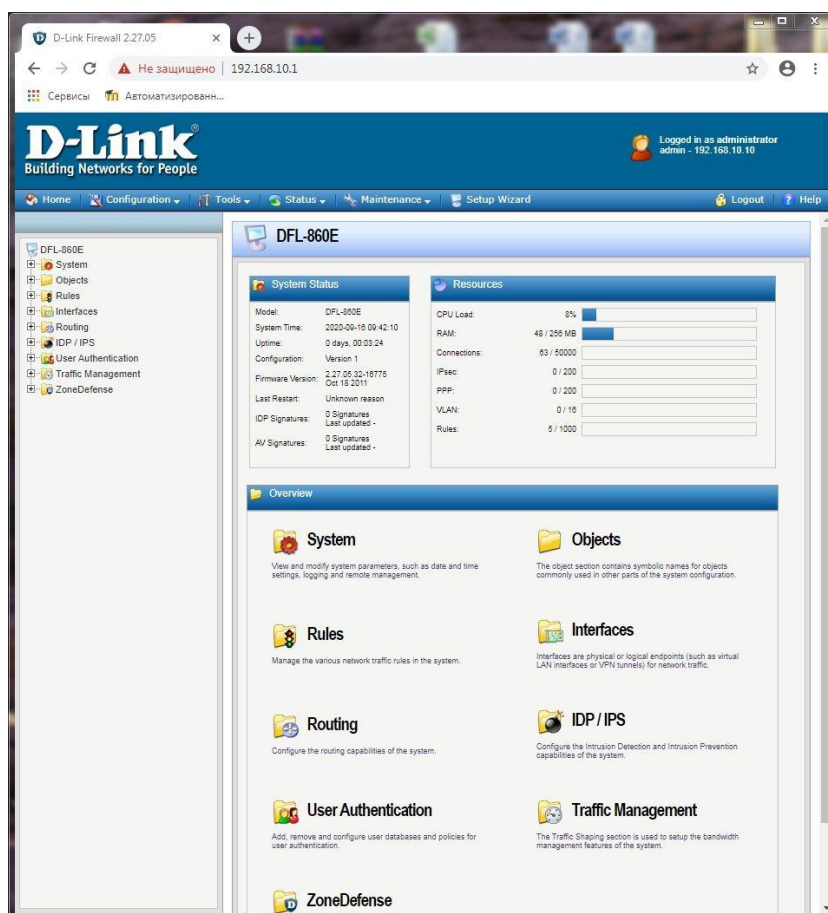
*Гомель 2020*

# Лабораторная работа №1

**Цель работы:** Рассмотреть общие вопросы администрирования межсетевого экрана.

1. Вход с использованием различных интерфейсов в консоль управление межсетевым экраном.
2. Перезапуск межсетевого экрана, сброс к заводским настройкам по умолчанию, установке даты и времени, DNS, активация и применение изменений.
3. Сброс и загрузка новой конфигурации устройства, автоматическое обновление ПО.
4. Поиск неисправностей.

Шаг 1. Для первоначального доступа к веб-интерфейсу межсетевого экрана с заводскими настройками по умолчанию следует использовать URL <https://192.168.10.1>. После этого появится диалоговое окно аутентификации пользователя. Далее попадаем на главную страницу настройки межсетевого экрана.



Шаг 2. По умолчанию, доступ к веб-интерфейсу открыт только из внутренней сети. Если необходимо включить доступ с других интерфейсов, кроме интерфейса lan, требуется изменить политику удаленного управления.

D-Link Firewall 2.27.05

← → ↻ Не защищено | 192.168.10.1

Сервисы Автоматизированн...

# D-Link®

Building Networks for People

Logged in as administrator  
admin - 192.168.10.10

Home Configuration Tools Status Maintenance Setup Wizard Logout Help

DFL-860E

- System
  - Date and Time
  - DNS
  - Remote Management
  - Log and Event Receivers
  - DHCP
  - Misc. Clients
  - Hardware Monitoring
  - Whitelist
  - Advanced Settings
- Objects
- Rules
- Interfaces
- Routing
- IDP / IPS
- User Authentication
- Traffic Management
- ZoneDefense

## HTTP/HTTPS Management

Configure HTTP/HTTPS management to enable remote management to the system.

General

**Remote Access Type**

Name: RemoteMgmtHTTP

☒ HTTP

☒ HTTPS

**Access**

Select the user database to use for login and the access level to grant to the user.

User Database: AdminUsers

Access Level: Admin

**Access Filter**

Remote access is granted from the following interface and network.

Interface: any

Network: all-nets

**Comments**

Comments:

OK Cancel

## Remote Management

Setup and configure methods and permissions for remote management of this system.

Add Advanced Settings

#	Name	Type	Mode	Interface	Network	Comments
1	RemoteMgmtHTTP	HTTP/HTTPS Management	Admin: HTTPS	lan	lannet	
2	RemoteMgmtHTTP_k	HTTP/HTTPS Management	Admin: HTTP, HTTPS	any	all-nets	

Right-click on a row for additional options.

Шаг 3. Система NetDefendOS поддерживает версии 1, 1.5 и 2 протокола SSH. Разрешение доступа по протоколу SSH предоставляется с помощью политики удалённого управления, и по умолчанию разрешения доступа по протоколу SSH нет.

**SSH\_lan**  
Configure a Secure Shell (SSH) Server to enable remote management access to the system.

**General**

Name: SSH\_lan

Listening Port: 22

Max Concurrent Clients: 5

Session idle timeout: 1800

Login grace timeout: 30

Greeting Message:

Maximum Authentication Retries: 3

**Authentication Methods**

Client authentication methods that this server supports

Password: ☒

Public Key: ☒

**Host Key Algorithms**

Public Key Algorithms for which the unit has private host keys stored. These are also the algorithms that the server supports for clients that uses Public Key authentication.

DSA: ☒

RSA: ☒

**Key Exchange Algorithms**

AES-128 ☒ AES-192 ☒

3DES ☒ AES-256 ☒

**Integrity Algorithms**

SHA1 ☒ MD5 ☒

SHA1-96 ☒ MD5-96 ☒

**Access**

Select the user database to use for login and the access level to grant to the user.

User Database: AdminUsers

Access Level: Admin

Шаг 4. После первоначального запуска рекомендуется как можно скорее изменить пароль по умолчанию admin на любой другой. Пароль пользователя может быть любой комбинацией символов и не может содержать более 256 СИМВОЛОВ.

**admin**  
User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec XAuth, Web Authentication, etc

General SSH Public Key

**General**

Name: admin

Password: ..... Note! Existing passwords will always be shown with 8 characters to hide the actual length.

Confirm Password: .....

Groups: administrators

Comma separated list of groups  
Users that are members of the 'administrators' group are allowed to change the firewall configuration.  
Users that are members of the 'auditors' group are only allowed to view the firewall configuration.

Add administrators Add auditors

**Per-user PPTP/L2TP IP Configuration**

Static Client IP Address: (None)

Networks behind user: (None)

Metric for networks:

**Comments**

Comments:

OK Cancel

Шаг 5. Установить дату и время можно вручную, это рекомендуется при первоначальном запуске системы.

192.168.10.1

D-Link Firewall 2.27.05 - Google Chrome

Не защищено | 192.168.10.1/?Page=DateTimeSet

### Set Date and Time

Date: 2020 - Sep - 16

Time: 10:12:53 (HH:MM:SS)

OK Cancel

---

### Date and Time

Set the date, time and time zone information

General

General

Current Date and Time: 2020-09-16 10:11:58 Set Date and Time

### Time zone and daylight saving time settings

Time zone: (GMT+03:00)

☐ Enable daylight saving time

Offset: 60 minutes

Start Date: March 1

End Date: October 1

### Automatic time synchronization

☒ Disabled

☐ D-Link (pre-configured timesync server)

☐ Custom

Time Server Type: SNTP

Primary Time Server: (None)

Secondary Time Server: (None)

Tertiary Time Server: (None)

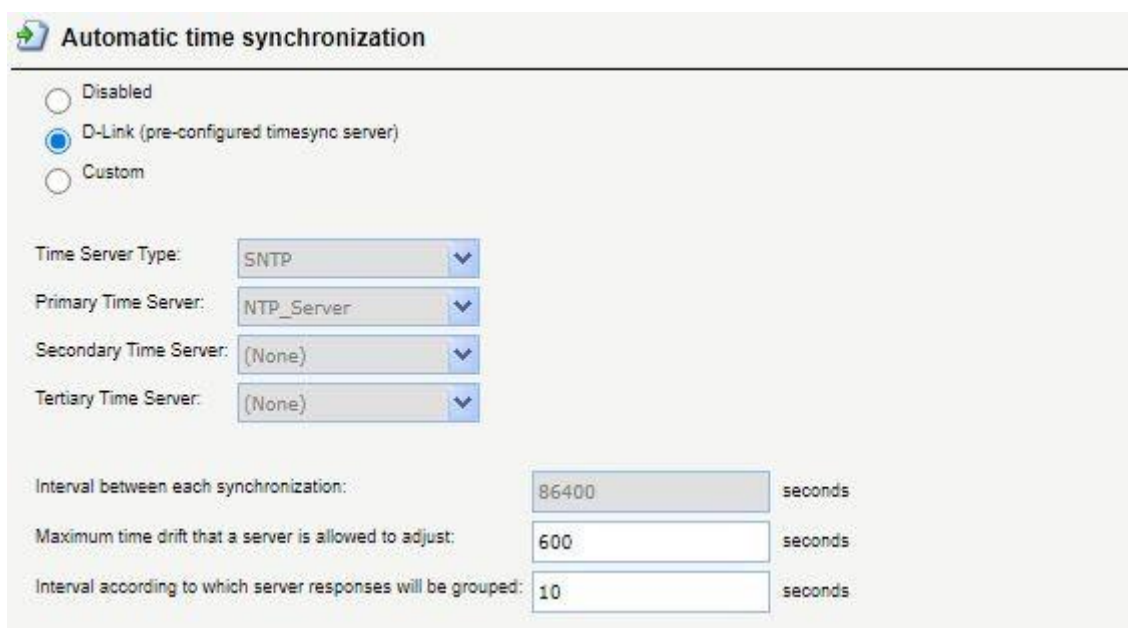
Interval between each synchronization: 86400 seconds

Maximum time drift that a server is allowed to adjust: 600 seconds

Interval according to which server responses will be grouped: 10 seconds

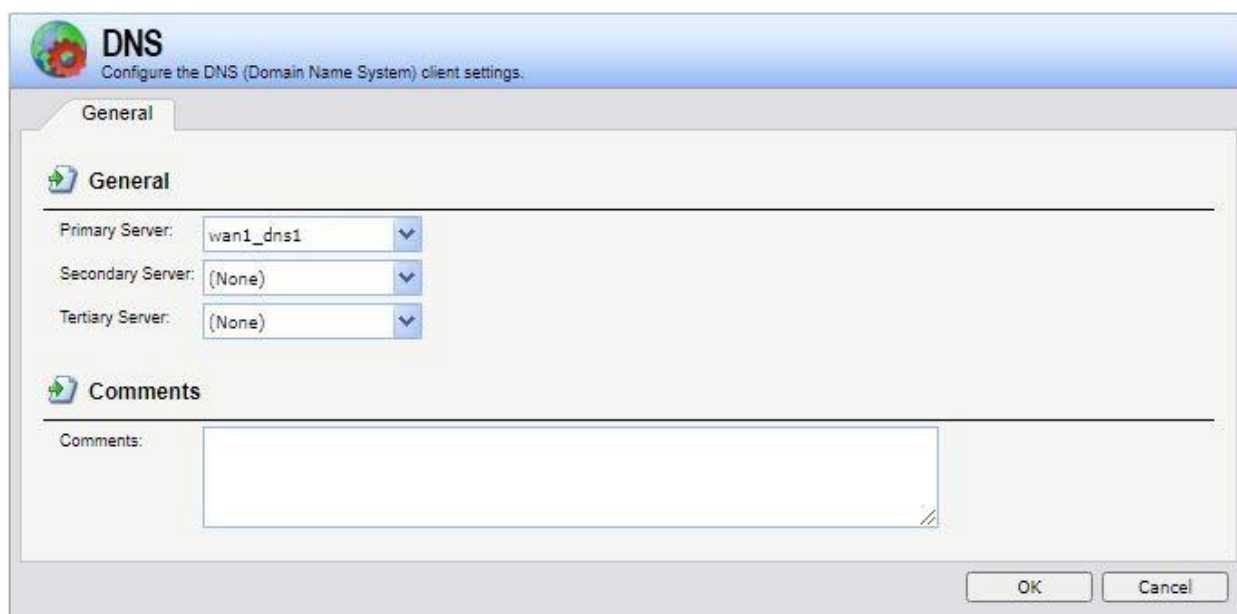
OK Cancel

Шаг 6. Чтобы избежать установления некорректного времени, которое может произойти при синхронизации с неисправным сервером, можно установить максимальную величину корректирования времени.



The image shows a window titled "Automatic time synchronization" with a green arrow icon. It contains three radio buttons: "Disabled", "D-Link (pre-configured timesync server)" (which is selected), and "Custom". Below these are four dropdown menus for "Time Server Type" (set to "SNTP"), "Primary Time Server" (set to "NTP\_Server"), "Secondary Time Server" (set to "(None)"), and "Tertiary Time Server" (set to "(None)"). At the bottom, there are three input fields with "seconds" labels: "Interval between each synchronization:" (86400), "Maximum time drift that a server is allowed to adjust:" (600), and "Interval according to which server responses will be grouped:" (10).


Шаг 7. Если в системе настроены DNS-сервера, то вместо IP-адреса можно указывать соответствующее доменное имя. Система NetDefendOS является DNS-клиентом и может использовать три DNS-сервера: Primary Server (первичный сервер), Secondary server (вторичный сервер) и Tertiary server (третий сервер).



The image shows a window titled "DNS" with a gear icon and the subtitle "Configure the DNS (Domain Name System) client settings." It has a "General" tab selected. Under the "General" section, there are three dropdown menus for "Primary Server" (set to "wan1\_dns1"), "Secondary Server" (set to "(None)"), and "Tertiary Server" (set to "(None)"). Below this is a "Comments" section with a text area. At the bottom right are "OK" and "Cancel" buttons.




Шаг 8. Сброс к заводским настройкам по умолчанию выполняется для возврата к первоначальным настройкам межсетевого экрана. При выполнении сброса настроек все данные, такие, как база данных провайдера и антивирусная база данных, будут утеряны и должны быть повторно загружены.



## Reset


This will restore components to factory defaults. This means that all configuration parameters will be wiped. On the next start-up, its LAN IP address will be 192.168.1.1, and the web GUI will begin with the setup wizard. It will not accept connections on any interface other than the LAN interface.



### Restart

- ☐ Reconfigure - Re-read configuration.
- ☒ Restart - Restart, but first wait for all subsystems to shutdown gracefully.
- ☐ Reboot - Power-off directly and restart from power-on state.

Restart the unit



### Reset to Factory Defaults

- ☒ Restore the configuration to factory default.
- ☐ Restore the entire unit to factory defaults. This includes firmware version, IDP signatures and configuration.

Reset to Factory Defaults