Гомельский Государственный Университет
им. Ф. Скорины

Лабораторный практикум №1. Основы администрирования межсетевого экрана D-Link DFL-860

Проверил:
Грищенко В.В.

Студент МС – 42:
Кузнецов Ю.В.

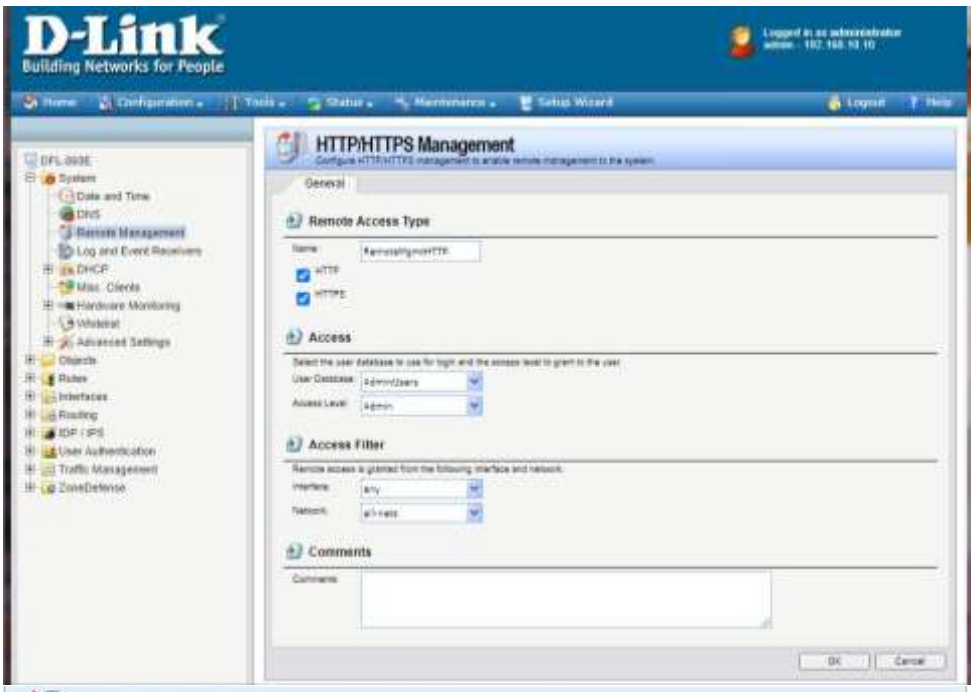
г. Гомель

Цель работы: рассмотрим общие вопросы администрирования межсетевого экрана.

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

Постановка задачи:

Последовательность действий



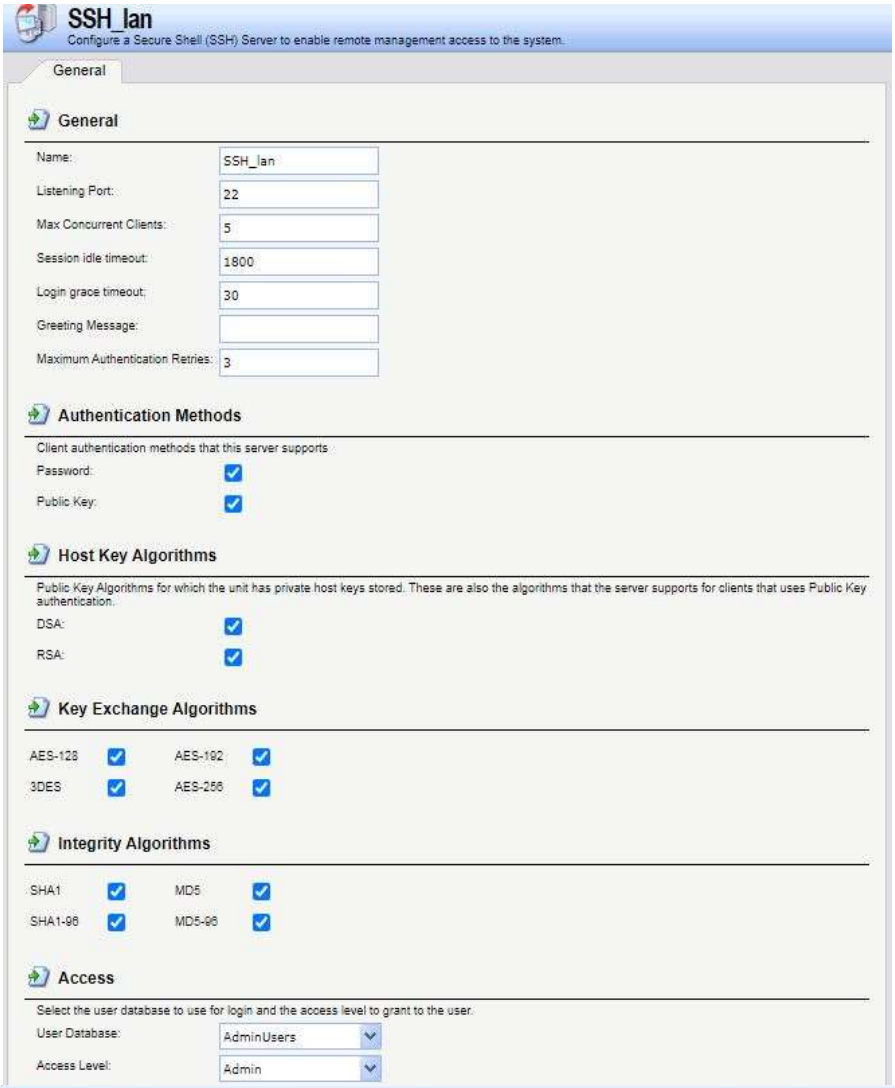
Remote Management

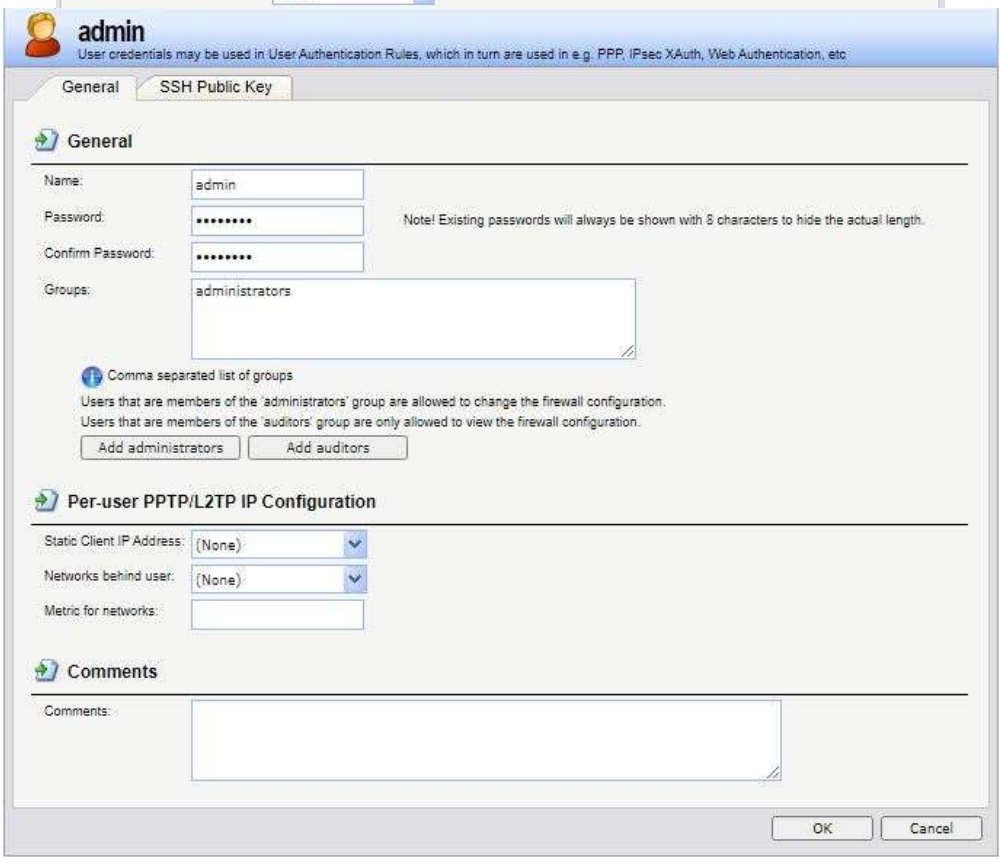
Setup and configure methods and permissions for remote management of this system.

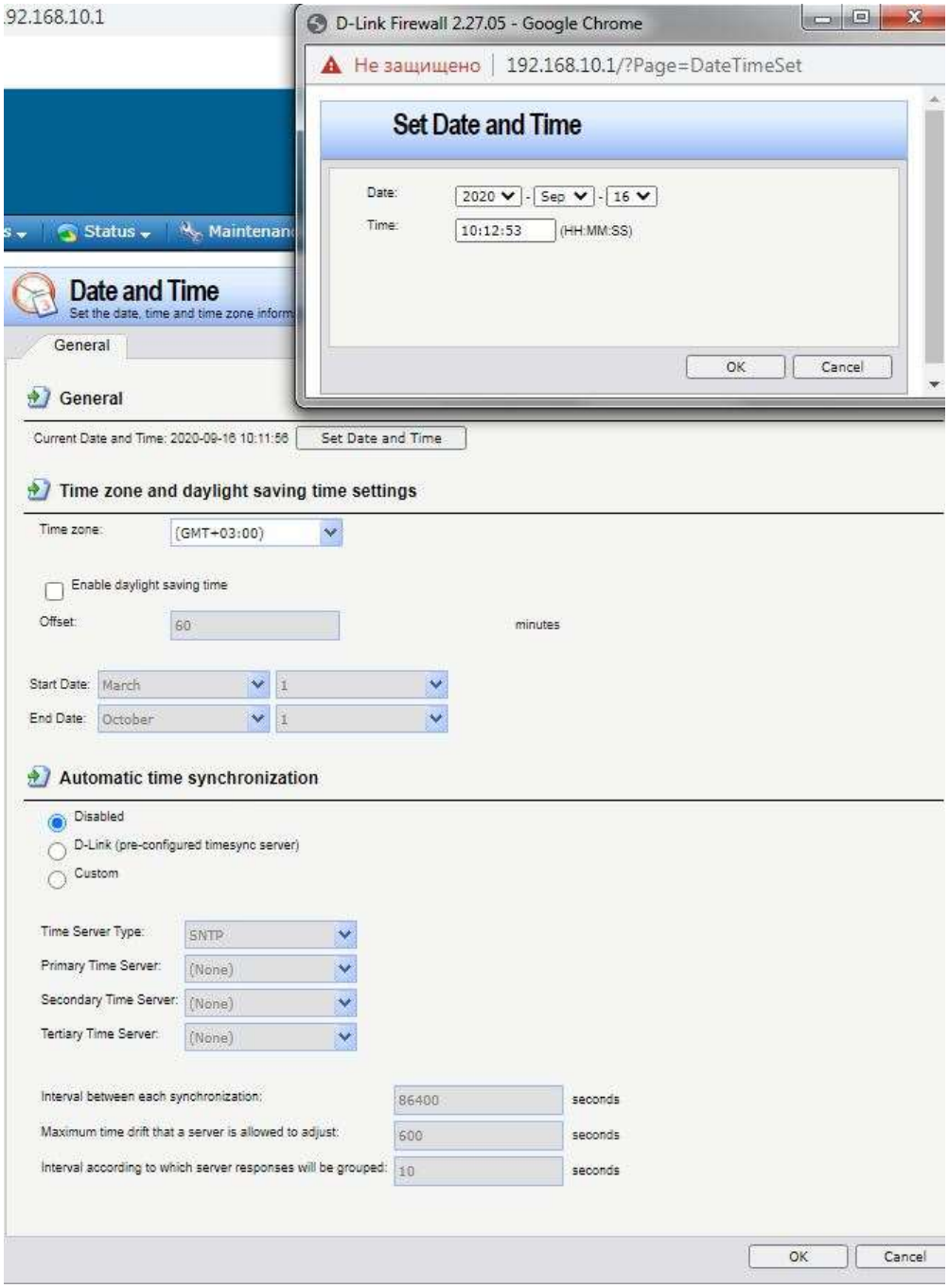
Add | Advanced Settings

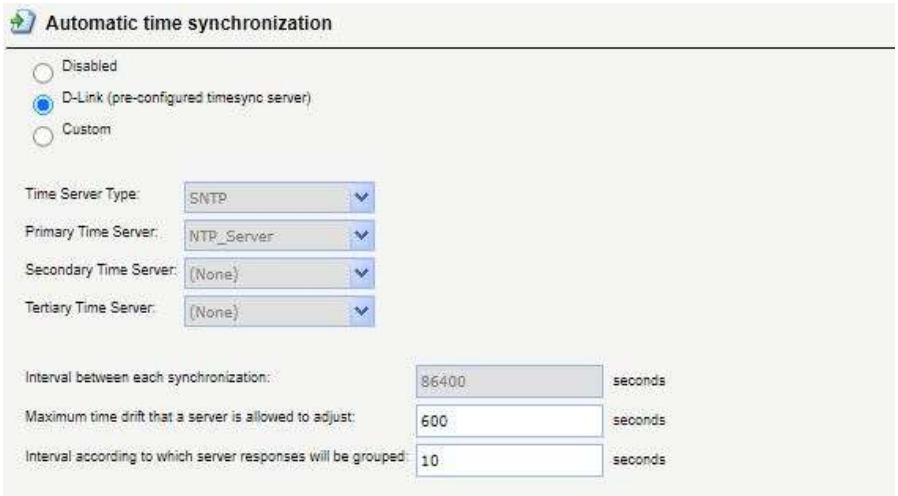
#	Name	Type	Mode	Interface	Network	Comments
1	RemoteMgmtHTTP	HTTP/HTTPS Management	Admin: HTTPS	lan	lannet	
2	RemoteMgmtHTTP_k	HTTP/HTTPS Management	Admin: HTTP, HTTPS	any	all-nets	

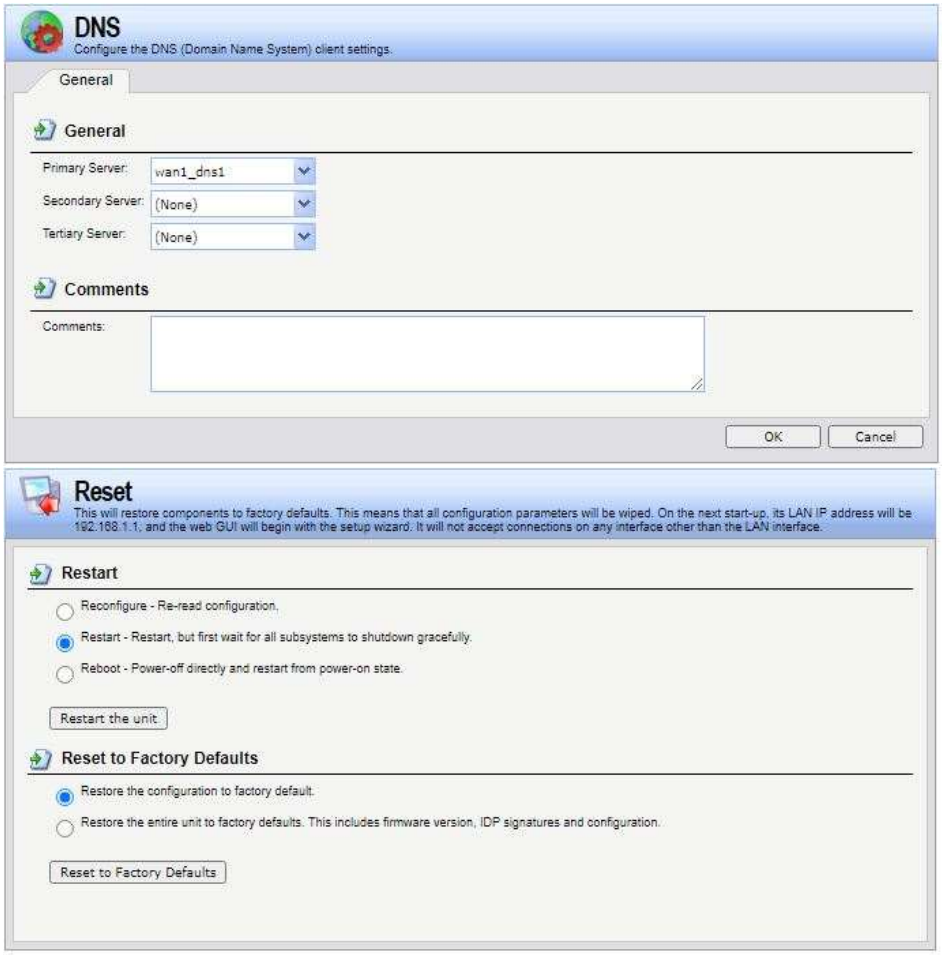
Right-click on a row for additional options.


SSH_lan
Configure a Secure Shell (SSH) Server to enable remote management access to the system.
General
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


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


92.168.10.1
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
Status
Maintenan
Date and Time
Set the date, time and time zone inform
General
General
Current Date and Time: 2020-09-16 10:11:56
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


Automatic time synchronization
Disabled
D-Link (pre-configured timesync server)
Custom
Time Server Type: SNTP
Primary Time Server: NTP_Server
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


DNS
Configure the DNS (Domain Name System) client settings.
General
General
Primary Server:
wan1_dns1
Secondary Server:
(None)
Tertiary Server:
(None)
Comments
Comments:
OK
Cancel
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