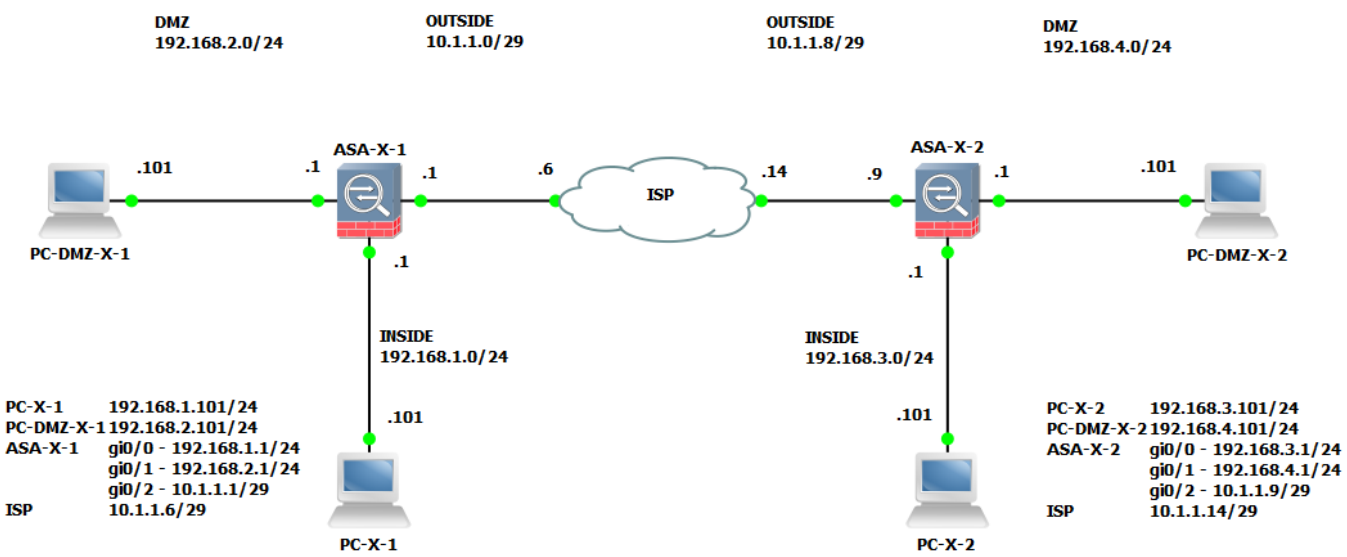
CCNA Security

Лабораторная работа 19

Настройка основных параметров Cisco ASA

Топология



Описание

В этой лабораторной работе вы познакомитесь с командной строкой Cisco ASA и настроите основные параметры.

Таблица адресации

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Имя (для команды nameif)	Security Level
ASA-X-1	G0/0	192.168.1.1/24	inside	100
	G0/1	192.168.2.1/24	dmz	50
	G0/2	10.1.1.1/29	outside	0
ASA-X-2	G0/0	192.168.3.1/24	inside	100
	G0/1	192.168.4.1/24	dmz	50
	G0/2	10.1.1.9/29	outside	0

Устройство	Интерфейс	IPv4-адрес/Маска подсети	Шлюз по умолчанию	DNS-сервер
PC-X-1	NIC	192.168.1.101/24	192.168.1.1	10.1.1.6
PC-DMZ-X-1	NIC	192.168.2.101/24	192.168.2.1	10.1.1.6
PC-X-2	NIC	192.168.3.101/24	192.168.3.1	10.1.1.14
PC-DMZ-X-2	NIC	192.168.4.101/24	192.168.4.1	10.1.1.14

Имена пользователей и пароли

	Console		SSH		Enable
Устройство	Имя пользователя	Пароль	Имя пользователя	Пароль	Пароль
ASA-X-1	-	-	-	-	-
ASA-X-2	-	-	-	-	-

Устройство	Имя пользователя	Пароль
PC-X-1	Student1	1
PC-DMZ-X-1	Student1	1
PC-X-2	Student1	1
PC-DMZ-X-2	Student1	1

Часть 1: Просмотр и настройка основных параметров

1. Уточните у преподавателя номер вашей группы и месторасположение в топологии (слева или справа). По ходу лабораторной работы изменяйте в командах параметр **X** на номер вашей группы. Параметры для левой или правой стороны могут отличаться.
   Номер группы: _____
   Месторасположение: _____

   ```
   Здесь будут написаны команды для обеих сторон.
   ```

Здесь будут написаны команды для левой стороны.	Здесь будут написаны команды для правой стороны.

2. Подключитесь к консоли ASA.

3. Вы попали в пользовательский (или непривилегированный) режим. Как и раньше можно пользоваться контекстной справкой (спасительный значок «**?**»). Посмотрите все доступные команды.
   ```
   ciscoasa> ?

     clear       Reset functions
     enable      Turn on privileged commands
     exit        Exit from the EXEC
     help        Interactive help for commands
     login       Log in as a particular user
     logout      Exit from the EXEC
     no          Negate a command or set its defaults
     ping        Send echo messages
     quit        Exit from the EXEC
     show        Show running system information
     traceroute  Trace route to destination
   ciscoasa>
   ```

4. Посмотрите список параметров у команды **ping**.
   ```
   ciscoasa> ping ?

     Hostname or A.B.C.D     Ping destination IPv4 address or hostname
     Hostname or X:X:X:X::X  Ping destination IPv6 address or hostname
     <cr>
   ```

5. Новая команда **help** позволяет посмотреть большее количество справочной информации о командах и параметрах. Чем-то команда **help** напоминает команду **man** в системах Linux.
   ```
   ciscoasa> help ping

   USAGE:

           ping {tcp [if_name] <host> <port>
   ```

```
                [repeat <count>] [timeout <seconds>] [source <host> <port>] |
                [if_name] <host> [repeat <count>] [timeout <seconds>]
                [data <pattern>] [size <bytes>] [validate]}

        Note: 'data', 'size', and 'validate' options not
        available with 'tcp' option; 'source' and
        '<port>' options only available with 'tcp' option.

DESCRIPTION:

ping            Test connectivity from specified interface to an IP address

SYNTAX:

[tcp]           Specify TCP instead of ICMP for ping session.

[if_name]       ICMP: The interface name, as specified by the 'nameif' command,
                by which <host> is accessible.  If not supplied, then <host>
                is resolved to an IP address and then the routing table
                is consulted to determine the destination interface.
                TCP: The input interface name through which the source
                will send SYN packets.

<host>          IPv4 address, IPv6 address or name of host to ping.

<port>          Associated port number 1-65535.

[source]        Specify a certain IP address and port to send from
                (Use port = '0' for a random port).

<pattern>       16 bit data pattern in hex.

<count>         Repeat count.

<bytes>         Datagram size in bytes.

<seconds>       Timeout in seconds.

validate        Validate reply data.
```

6. Войдите в привилегированный режим. По умолчанию пароль для входа в привилегированный режим не установлен, просто нажмите Enter.

```
ciscoasa> enable
Password: < Нажмите Enter >
ciscoasa#
```

7. Посмотрите основную информацию об устройстве. Вы увидите версию ПО ASA, версию графической оболочки ASDM, модель устройства, тип и объём памяти, информацию об интерфейсах, параметры лицензии.

```
ciscoasa# show version

Cisco Adaptive Security Appliance Software Version 9.5(2)10
Device Manager Version 7.5(2)

Compiled on Wed 25-May-16 17:41 PDT by builders
System image file is "boot:/asa952-10-smp-k8.bin"
Config file at boot was "startup-config"
```

```
ciscoasa up 5 mins 56 secs

Hardware:   ASAv, 1024 MB RAM, CPU Xeon 5500 series 3392 MHz,
Model Id:   ASAv5
Internal ATA Compact Flash, 256MB
Slot 1: ATA Compact Flash, 8192MB
BIOS Flash Firmware Hub @ 0x0, 0KB


 0: Ext: Management0/0        : address is 000c.29aa.122d, irq 10
 1: Ext: GigabitEthernet0/0   : address is 000c.29aa.1237, irq 5
 2: Ext: GigabitEthernet0/1   : address is 000c.29aa.1241, irq 9
 3: Ext: GigabitEthernet0/2   : address is 000c.29aa.124b, irq 11

< Вывод опущен >

Licensed features for this platform:
Maximum Physical Interfaces       : 10
Maximum VLANs                     : 25
Inside Hosts                      : Unlimited
Failover                          : Active/Standby
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 0
Carrier                           : Disabled
AnyConnect Premium Peers          : 2
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 50
Total VPN Peers                   : 50
AnyConnect for Mobile             : Disabled
AnyConnect for Cisco VPN Phone    : Disabled
Advanced Endpoint Assessment      : Disabled
Shared License                    : Disabled
Total UC Proxy Sessions           : 2
Botnet Traffic Filter             : Enabled
Cluster                           : Disabled

< Вывод опущен >
```

8. Посмотрите содержимое файла **startup-config**. Стартовая конфигурация отсутствует.
```
ciscoasa# show start
No Configuration
```

9. Посмотрите краткую информацию обо всех интерфейсах. Обратите внимание, что команда несколько изменилась, параметры interface и ip поменялись местами. Как и на маршрутизаторе, все интерфейсы по умолчанию выключены.
```
ciscoasa# show interface ip brief
Interface                  IP-Address   OK? Method Status                Protocol
GigabitEthernet0/0         unassigned   YES unset  administratively down up
```

```
GigabitEthernet0/1         unassigned   YES unset  administratively down up
GigabitEthernet0/2         unassigned   YES unset  administratively down up
Management0/0              unassigned   YES unset  administratively down down
```

10. Посмотрите более подробную информацию об интерфейсе g0/0.

```
ciscoasa# show int g0/0
Interface GigabitEthernet0/0 "", is administratively down, line protocol is up
  Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address 000c.29aa.1237, MTU not set
        IP address unassigned
        12 packets input, 4053 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
```

11. Войдите в режим конфигурирования. Откажитесь от отправки анонимной статистики.

```
ciscoasa# conf t

***************************** NOTICE *****************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: < Введите N, потом нажмите Enter >

In the future, if you would like to enable this feature,
Issue the command "call-home reporting anonymous".

Please remember to save your configuration.

ciscoasa(config)#
```

12. Измените имя устройства. Вместо X поставьте номер вашей группы.

`ciscoasa(config)# hostname ASA-X-1` `ASA-X-1(config)#`	`ciscoasa(config)# hostname ASA-X-2` `ASA-X-2(config)#`

13. Измените имя домена.

```
ASA-X-1(config)# domain-name acad.local
```

14. Задайте пароль на привилегированный режим. В Cisco ASA более нет параметра secret, только password. Однако пароль, заданный с помощью параметра password, будет храниться в конфигурации в шифрованном виде.

```
ASA-X-1(config)# enable password cisco12345
```

15. Выведите кусочек текущей конфигурации, а конкретно только строки, содержащие слово password. Помните, что более не нужно использовать команду do, можно использовать команды show, ping, traceroute и другие находясь в любом режиме.

```
ASA-X-1(config)# show run | i password
enable password 9D8jmmmgkfNZLETh encrypted
```

16. Добавьте баннер MOTD.

```
ASA-X-1(config)# banner motd Unauthorized access strictly prohibited!
ASA-X-1(config)# exit
```

17. Проверьте проведённые настройки.

```
ASA-X-1# exit

Logoff

Unauthorized access strictly prohibited!
Type help or '?' for a list of available commands.
ASA-X-1> enable
Password: < Введите cisco12345, потом нажмите Enter >
ASA-X-1#
```

18. Сохраните конфигурацию.

```
ASA-X-1# copy run start

Source filename [running-config]? < Нажмите Enter >
Cryptochecksum: 4845bb6d 40597179 ed939c5c 7b821db1

6535 bytes copied in 0.190 secs
ASA-X-1#
```

19. Выведите содержимое файла **startup-config**. Бегло окиньте файл взглядом, найдите те параметры, которые вы меняли.

```
ASA-X-1# show start
< Вывод опущен >
hostname ASA-3-1
domain-name acad.local
enable password 9D8jmmmgkfNZLETh encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
```

```
!
interface GigabitEthernet0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
< Вывод опущен >
```

20. Перезагрузите устройство.

```
ASA-X-1# reload
Proceed with reload? [confirm] < Нажмите Enter >
```

21. Дождитесь загрузки. Удостоверьтесь, что ваши настройки сохранились.

```
< Вывод опущен >

Unauthorized access strictly prohibited!
Type help or '?' for a list of available commands.
ASA-X-1> enable
Password: < Введите cisco12345, потом нажмите Enter >
ASA-X-1#
```

Часть 2: Настройка интерфейсов

1. Войдите в режим конфигурирования.
```
ASA-X-1# conf t
ASA-X-1(config)#
```

2. Войдите в режим конфигурирования интерфейса g0/0.
```
ASA-X-1(config)# int g0/0
ASA-X-1(config-if)#
```

3. Назначьте IPv4-адрес и маску.

`ASA-X-1(config-if)# ip addr 192.168.1.1 255.255.255.0`	`ASA-X-2(config-if)# ip addr 192.168.3.1 255.255.255.0`

4. Обязательно назначьте имя с помощью команды **nameif**. Даже если у вас назначены адрес и маска, интерфейс включён, без имени интерфейс работать не будет.
```
ASA-X-1(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
```

5. Хотя интерфейсу автоматически был присвоен уровень безопасности 100, назначьте уровень безопасности ещё раз, чтобы познакомиться с командой.
```
ASA-X-1(config-if)# security-level 100
```

6. Включите интерфейс. Сообщения о включении интерфейса не будет, в этом плане Cisco ASA более молчалива.
```
ASA-X-1(config-if)# no shut
ASA-X-1(config-if)# exit
```

7. Посмотрите краткую информацию обо всех интерфейсах. Ниже представлен вывод для левой части топологии.
```
ASA-X-1(config)# show int ip br
Interface                  IP-Address    OK? Method Status                Protocol
GigabitEthernet0/0         192.168.1.1   YES manual up                    up
GigabitEthernet0/1         unassigned    YES unset  administratively down up
GigabitEthernet0/2         unassigned    YES unset  administratively down up
Management0/0              unassigned    YES unset  administratively down down
```

8. Посмотрите подробную информацию об интерфейсе g0/0. Ниже представлен вывод для левой части топологии.
```
ASA-X-1(config)# show int g0/0
Interface GigabitEthernet0/0 "inside", is up, line protocol is up
  Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address 000c.29aa.1237, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        68 packets input, 22744 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
        0 pause input, 0 resume input
        0 L2 decode drops
        1 packets output, 60 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 2 interface resets
        0 late collisions, 0 deferred
        60 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (503/503)
        output queue (blocks free curr/low): hardware (511/510)
    Traffic Statistics for "inside":
        8 packets input, 2624 bytes
        1 packets output, 28 bytes
        8 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  4 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

9. Настройте интерфейс g0/1: присвойте IPv4-адрес, маску, имя, уровень безопасности, включите интерфейс.

ASA-X-1(config)# **int g0/1**	ASA-X-2(config)# **int g0/1**
ASA-X-1(config-if)# **ip addr 192.168.2.1 255.255.255.0**	ASA-X-2(config-if)# **ip addr 192.168.4.1 255.255.255.0**
ASA-X-1(config-if)# **nameif dmz**	ASA-X-2(config-if)# **nameif dmz**
ASA-X-1(config-if)# **security-level 50**	ASA-X-2(config-if)# **security-level 50**
ASA-X-1(config-if)# **no shut**	ASA-X-2(config-if)# **no shut**
ASA-X-1(config-if)# **exit**	ASA-X-2(config-if)# **exit**

10. Настройте интерфейс g0/2: присвойте IPv4-адрес, маску, имя, уровень безопасности, включите интерфейс.

ASA-X-1(config)# **int g0/2**	ASA-X-2(config)# **int g0/2**
ASA-X-1(config-if)# **ip addr 10.1.1.1 255.255.255.248**	ASA-X-2(config-if)# **ip addr 10.1.1.9 255.255.255.248**
ASA-X-1(config-if)# **nameif outside**	ASA-X-2(config-if)# **nameif outside**
ASA-X-1(config-if)# **security-level 0**	ASA-X-2(config-if)# **security-level 0**
ASA-X-1(config-if)# **no shut**	ASA-X-2(config-if)# **no shut**
ASA-X-1(config-if)# **exit**	ASA-X-2(config-if)# **exit**

11. Посмотрите краткую информацию обо всех интерфейсах. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show int ip br
Interface                  IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0         192.168.1.1     YES manual up                    up
GigabitEthernet0/1         192.168.2.1     YES manual up                    up
GigabitEthernet0/2         10.1.1.1        YES manual up                    up
Management0/0              unassigned      YES unset  administratively down down
```

12. Посмотрите подробную информацию об интерфейсах g0/1 и g0/2. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show int g0/1
Interface GigabitEthernet0/1 "dmz", is up, line protocol is up
  Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address 000c.29aa.1241, MTU 1500
        IP address 192.168.2.1, subnet mask 255.255.255.0
< Вывод опущен >

ASA-X-1(config)# show int g0/2
Interface GigabitEthernet0/2 "outside", is up, line protocol is up
  Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address 000c.29aa.124b, MTU 1500
        IP address 10.1.1.1, subnet mask 255.255.255.248
< Вывод опущен >
```

13. Посмотрите краткую информацию обо всех интерфейсах, их именах и уровнях безопасности с помощью команды **show nameif**. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show nameif
Interface                      Name                           Security
GigabitEthernet0/0             inside                         100
GigabitEthernet0/1             dmz                            50
GigabitEthernet0/2             outside                        0
```

14. Посмотрите краткую информацию обо всех интерфейсах, их именах, адресах и масках с помощью команды **show ip addr**. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show ip addr
System IP Addresses:
Interface                      Name                           IP address      Subnet mask     Method
GigabitEthernet0/0             inside                         192.168.1.1     255.255.255.0   manual
GigabitEthernet0/1             dmz                            192.168.2.1     255.255.255.0   manual
GigabitEthernet0/2             outside                        10.1.1.1        255.255.255.248 manual

Current IP Addresses:
Interface                      Name                           IP address      Subnet mask     Method
GigabitEthernet0/0             inside                         192.168.1.1     255.255.255.0   manual
GigabitEthernet0/1             dmz                            192.168.2.1     255.255.255.0   manual
GigabitEthernet0/2             outside                        10.1.1.1        255.255.255.248 manual
```

15. Проверьте связь с провайдером с помощью команды **ping**. Проверка связи будет успешной.

`ASA-X-1(config)# ping 10.1.1.6`	`ASA-X-2(config)# ping 10.1.1.14`

16. Проверьте связь с сервером в сети Интернет с помощью команды **ping**. В качестве параметра укажите **адрес 8.8.8.8**. Проверка связи будет неуспешной, т.к. нет маршрута по умолчанию в таблице маршрутов. Позже вы это исправите.

```
ASA-X-1(config)# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
```

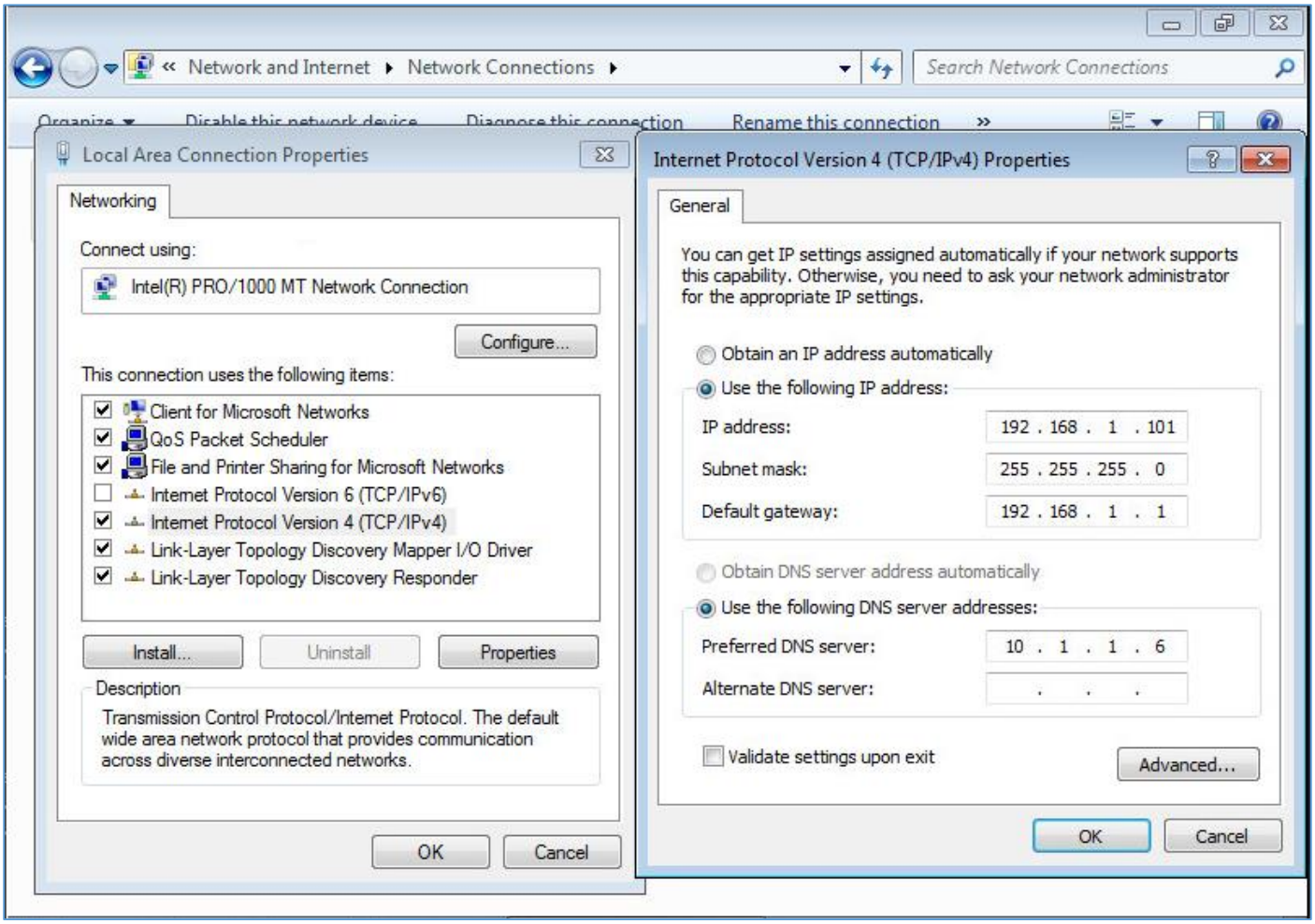
```
No route to host 8.8.8.8

Success rate is 0 percent (0/1)
```

17. Проверьте связь с сервером в сети Интернет с помощью команды **ping**. В качестве параметра укажите **доменное имя ya.ru**. Проверка связи будет неуспешной, т.к. на Cisco ASA не включено разрешение DNS-имён и не настроены адреса DNS-серверов. Позже вы это исправите.

```
ASA-X-1(config)# ping ya.ru
                  ^
ERROR: % Invalid Hostname
```

18. Перейдите в виртуальную машину PC (PC-X-1 или PC-X-2).

19. Назначьте IPv4-адрес, маску, адрес шлюза по умолчанию, адрес DNS-сервера согласно таблице адресации, расположенной в самом начале лабораторной работы. Ниже представлен пример для левой части топологии.



20. Откройте командую строку.

21. Проверьте связь с Cisco ASA с помощью команды **ping**. В качестве параметра укажите адрес Cisco ASA на **ближайшем** к PC интерфейсе (g0/0). Проверка связи будет успешной.

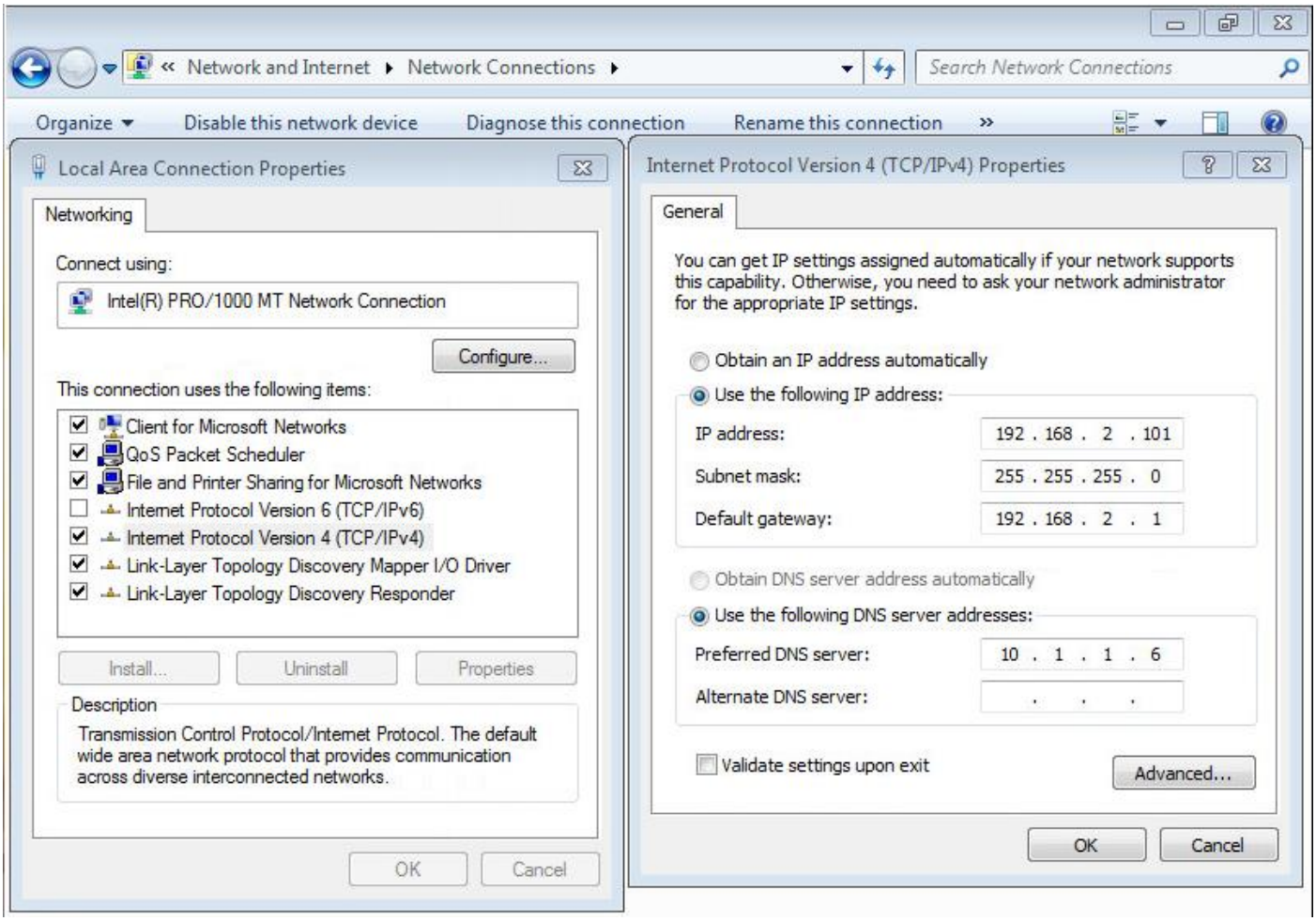
`C:\Users\Student1>` **`ping 192.168.1.1`**	`C:\Users\Student1>` **`ping 192.168.3.1`**

22. Проверьте связь с Cisco ASA с помощью команды **ping**. В качестве параметра укажите адрес Cisco ASA на **не ближайшем** к вам интерфейсе (например, g0/1). Проверка связи будет неуспешной. Это нормальное поведение. Запрещена любая связь с не ближайшим интерфейсом. Это поведение поменять нельзя.

`C:\Users\Student1>` **`ping 192.168.2.1`**	`C:\Users\Student1>` **`ping 192.168.4.1`**

23. Перейдите в виртуальную машину PC-DMZ (PC-DMZ-X-1 или PC-DMZ-X-2).

24. Назначьте IPv4-адрес, маску, адрес шлюза по умолчанию, адрес DNS-сервера согласно таблице адресации, расположенной в самом начале лабораторной работы. Ниже представлен пример для левой части топологии.



25. Откройте командую строку.

26. Проверьте связь с Cisco ASA с помощью команды **ping**. В качестве параметра укажите адрес Cisco ASA на **ближайшем** к PC-DMZ интерфейсе (g0/1). Проверка связи будет успешной.

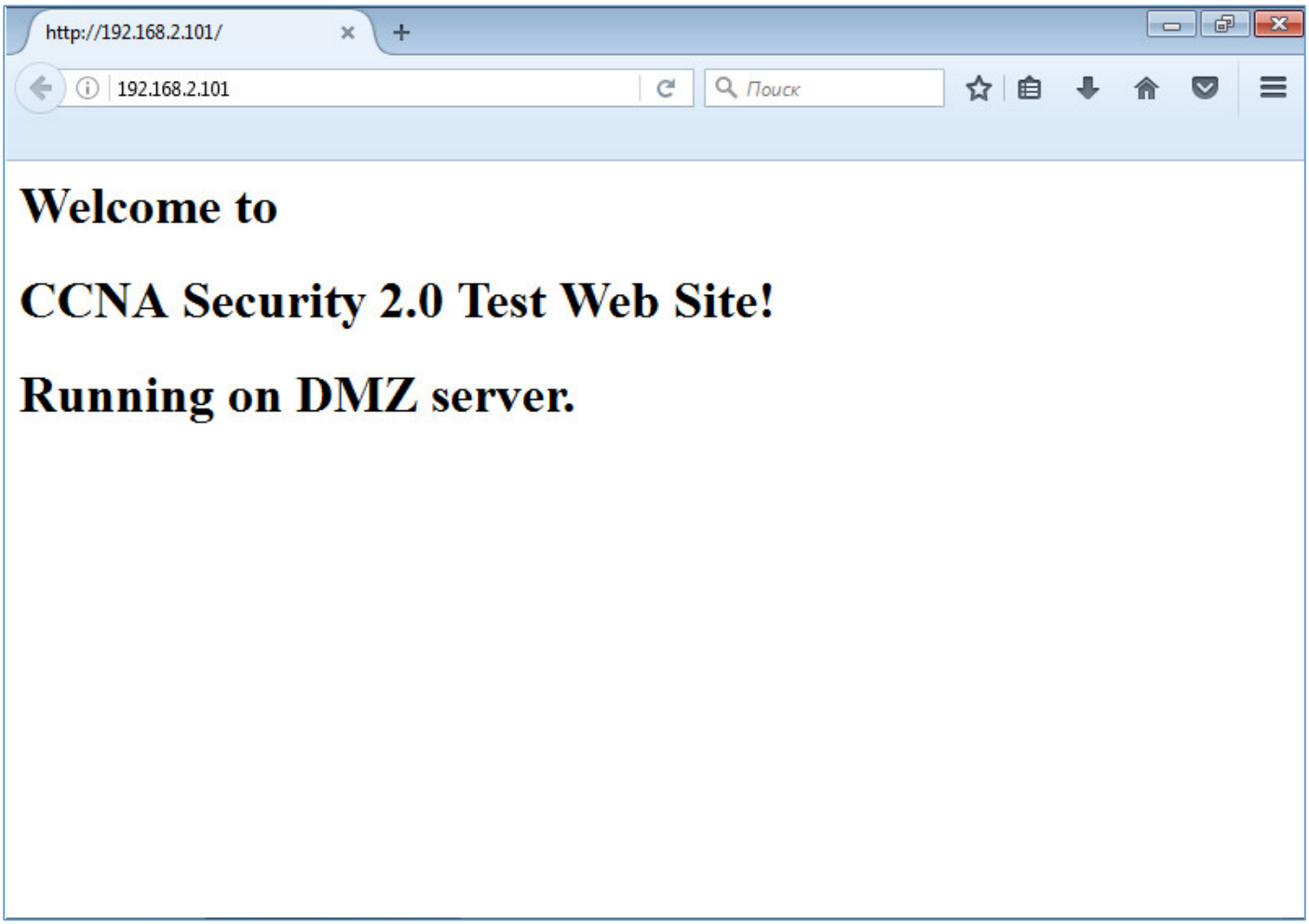
C:\Users\Student1> **ping 192.168.2.1**	C:\Users\Student1> **ping 192.168.4.1**

27. Вернитесь в виртуальную машину PC (PC-X-1 или PC-X-2).

28. Откройте браузер, попробуйте зайти на свой сервер PC-DMZ по протоколу http. Успешно откроется тестовая страница. Почему?

    - Траффик поступил на интерфейс g0/0. Cisco ASA ищет, куда переслать пакет, согласно таблице маршрутов. Сеть получателя доступна как напрямую подключённая, найден выходной интерфейс g0/1;
    - Траффик идёт с интерфейса с уровнем безопасности 100 на интерфейс с уровнем безопасности 50, из большего уровня в меньший. Значит это исходящий траффик, а исходящий траффик по умолчанию инспектируется: пакет разрешается, создаётся запись в таблице состояний, возвратный траффик будет автоматически разрешён.

    Ниже представлен пример для левой части топологии.



29. Откройте командную строку, проверьте связь со своим сервером PC-DMZ с помощью команды **ping**. Проверка связи будет неуспешна. Почему?

- Траффик поступил на интерфейс g0/0. Cisco ASA ищет, куда переслать пакет, согласно таблице маршрутов. Сеть получателя доступна как напрямую подключённая, найден выходной интерфейс g0/1;
- Траффик идёт с интерфейса с уровнем безопасности 100 на интерфейс с уровнем безопасности 50, из большего уровня в меньший. Значит это исходящий траффик, а исходящий траффик по умолчанию инспектируется. Однако конкретно протокол ICMP **не инспектируется**. Позже вы это исправите.

Часть 3: Настройка маршрутизации

1. Вернитесь в консоль ASA.

2. Посмотрите содержимое таблицы маршрутов. Вы увидите локальные и напрямую подключённые маршруты. Обратите внимание, что вместо названия интерфейсов в таблице маршрутов фигурирует имя, назначенное командой nameif. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is not set

C        10.1.1.0 255.255.255.248 is directly connected, outside
L        10.1.1.1 255.255.255.255 is directly connected, outside
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
C        192.168.2.0 255.255.255.0 is directly connected, dmz
L        192.168.2.1 255.255.255.255 is directly connected, dmz
```

3. Cisco ASA поддерживает статическую и динамическую маршрутизацию (протоколы BGP, EIGRP, OSPF, RIP). Добавьте статический маршрут по умолчанию. В качестве адреса следующего перехода укажите адрес маршрутизатора провайдера. Адрес и маску 0.0.0.0 можно сократить просто до 0. Имя интерфейса можно дополнять клавишей TAB или посмотреть в подсказке спасительным значком вопроса “?”.

ASA-X-1(config)# **route o<Нажмите Tab>** ASA-X-1(config)# **route outside 0 0 10.1.1.6**	ASA-X-2(config)# **route o<Нажмите Tab>** **ASA-X-2(config)# route outside 0 0 10.1.1.14**

4. Посмотрите содержимое таблицы маршрутов ещё раз. Ниже представлен вывод для левой части топологии.

```
ASA-X-1(config)# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 10.1.1.6 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.1.1.6, outside
C        10.1.1.0 255.255.255.248 is directly connected, outside
L        10.1.1.1 255.255.255.255 is directly connected, outside
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
C        192.168.2.0 255.255.255.0 is directly connected, dmz
L        192.168.2.1 255.255.255.255 is directly connected, dmz
```

5. Проверьте связь с сервером в сети Интернет с помощью команды **ping**. В качестве параметра укажите **адрес 8.8.8.8**. Проверка связи будет успешной, т.к. теперь есть статический маршрут по умолчанию в таблице маршрутов.

```
ASA-X-1(config)# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
20/24/30 ms
```

Часть 4: Настройка разрешения имён

1. Включите разрешение DNS-имён. DNS-запросы и ответы должны уходить в сторону провайдера (интерфейс outside).
   ```
   ASA-X-1(config)# dns domain-lookup outside
   ```

2. Добавьте адрес DNS-сервера провайдера.

`ASA-X-1(config)# dns name-server 10.1.1.6`	`ASA-X-2(config)# dns name-server 10.1.1.14`

3. Проверьте связь с сервером в сети Интернет с помощью команды **ping**. В качестве параметра укажите **доменное имя ya.ru**. Проверка связи будет успешной. Из-за особенностей лабораторного стенда возможно вам потребуется сделать несколько попыток.
   ```
   ASA-X-1(config)# ping ya.ru
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 87.250.250.242, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 10/14/20 ms
   ```

Часть 5: Настройка системного времени и протокола NTP

1. Посмотрите текущую дату и время. Дата и время будут похожи на реальные, т.к. виртуальная машина при включении берёт системную дату и время с гипервизора.

```
ASA-X-1(config)# show clock
12:38:18.309 UTC Mon Jan 11 2020

ASA-X-1(config)# show clock detail
12:38:25.104 UTC Mon Jan 11 2020
Time source is hardware calendar
```

2. Установите часовой пояс Московского региона (+3 часа по сравнению с UTC).

```
ASA-X-1(config)# clock timezone MSK +3
```

3. Проверьте текущую дату и время ещё раз. Время сместилось на три часа вперёд.

```
ASA-X-1(config)# show clock
15:43:01.929 MSK Mon Jan 11 2020

ASA-X-1(config)# show clock detail
15:43:29.619 MSK Mon Jan 11 2020
Time source is hardware calendar
UTC time is:  12:43:29 UTC Mon Jan 11 2020
```

4. Настройте синхронизацию с NTP-сервером. В качестве NTP-сервера используйте адрес маршрутизатора провайдера.

`ASA-X-1(config)# ntp server 10.1.1.6`	`ASA-X-2(config)# ntp server 10.1.1.14`

5. Проверьте настройки и состояние протокола NTP. Помните, что протокол NTP не отрабатывает мгновенно. Чем больше разница между временем клиента и сервера, тем дольше может продолжаться первоначальная синхронизация. Не обязательно ждать окончания синхронизации, можете переходить к следующей части задания. Ниже представлен пример для левой части топологии с непрошедшей синхронизацией.

```
ASA-X-1(config)# show ntp associations
     address         ref clock     st  when  poll reach  delay  offset    disp
~10.1.1.6          0.0.0.0          16     -    64    0     0.0    0.00  16000.
* master (synced), # master (unsynced), + selected, - candidate, ~ configured

ASA-X-1(config)# show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is 00000000.00000000 (09:28:16.000 MSK Thu Feb 7 2036)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
```

Часть 6: Настройка протокола SSH

1. Создайте пользователя admin с паролем cisco12345. Ещё раз напомню, в Cisco ASA более нет параметра secret, только password. Однако пароль, заданный с помощью параметра password, будет храниться в конфигурации в шифрованном виде.
```
ASA-X-1(config)# username admin password cisco12345
ASA-X-1(config)# show run | i username
username admin password Km9FNismGAXIMvno encrypted
```

2. На Cisco ASA новая модель AAA включена по умолчанию. Создайте список методов, который будет использоваться при подключении по протоколу SSH. Укажите один единственный метод LOCAL (аутентификация по локальной базе данных пользователей и паролей), слово LOCAL обязательно напишите целиком заглавными буквами. Список доступа автоматически прилепляется к удалённым подключениям по протоколу SSH. Также в Cisco ASA отсутствует понятие линий: VTY, Console и т.д.
```
ASA-X-1(config)# aaa authentication ssh console LOCAL
```

3. Сгенерируйте ключи RSA с длиной 2048 бит. Перезапишите имеющиеся ключи, если они имеются.
```
ASA-X-1(config)# crypto key generate rsa general-keys modulus 2048
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait…
ASA-X-1(config)#
```

4. Разрешите доступ по протоколу SSH из локальной сети. По умолчанию доступ запрещён с любого адреса. В Cisco ASA все маски только прямые.

`ASA-X-1(config)# ssh 192.168.1.0 255.255.255.0 inside`	`ASA-X-2(config)# ssh 192.168.3.0 255.255.255.0 inside`

5. Разрешите протокол SSH только 2-ой версии.
```
ASA-X-1(config)# ssh version 2
```

6. Проверьте настройки протокола SSH. Ниже представлен вывод для левой части топологии.
```
ASA-X-1(config)# show ssh
Timeout: 5 minutes
Version allowed: 2
192.168.1.0 255.255.255.0 inside
```

7. Перейдите в виртуальную машину PC (PC-X-1 или PC-X-2).

8. Запустите PuTTY. Подключитесь к ASA по протоколу SSH, а затем перейдите в привилегированный режим.

9. Посмотрите список текущих удалённых сессий по протоколу SSH.

```
ASA-X-1# show ssh sessions
SID   Client IP         Version     Mode  Encryption  Hmac  State              Username
0     192.168.1.101     2.0         IN    aes-256-ctr sha1  SessionStarted     admin
                                    OUT   aes-256-ctr sha1  SessionStarted     admin
```

10. Закройте PuTTY и вернитесь в консоль ASA.

Часть 7: Настройка DHCP-сервера

1. Cisco ASA может выступать в качестве DHCP-сервера. Единственное неудобство – невозможно настроить резервирование IPv4-адресов. Добавьте диапазон выдаваемых IPv4-адресов.

`ASA-X-1(config)# dhcpd address 192.168.1.51-192.168.1.99 inside`	`ASA-X-2(config)# dhcpd address 192.168.3.51-192.168.3.99 inside`

2. Настройте выдачу адреса DNS-сервера.

`ASA-X-1(config)# dhcpd dns 10.1.1.6 interface inside`	`ASA-X-2(config)# dhcpd dns 10.1.1.14 interface inside`

3. Настройте выдачу имени домена acad.local.
   `ASA-X-1(config)# dhcpd domain acad.local interface inside`

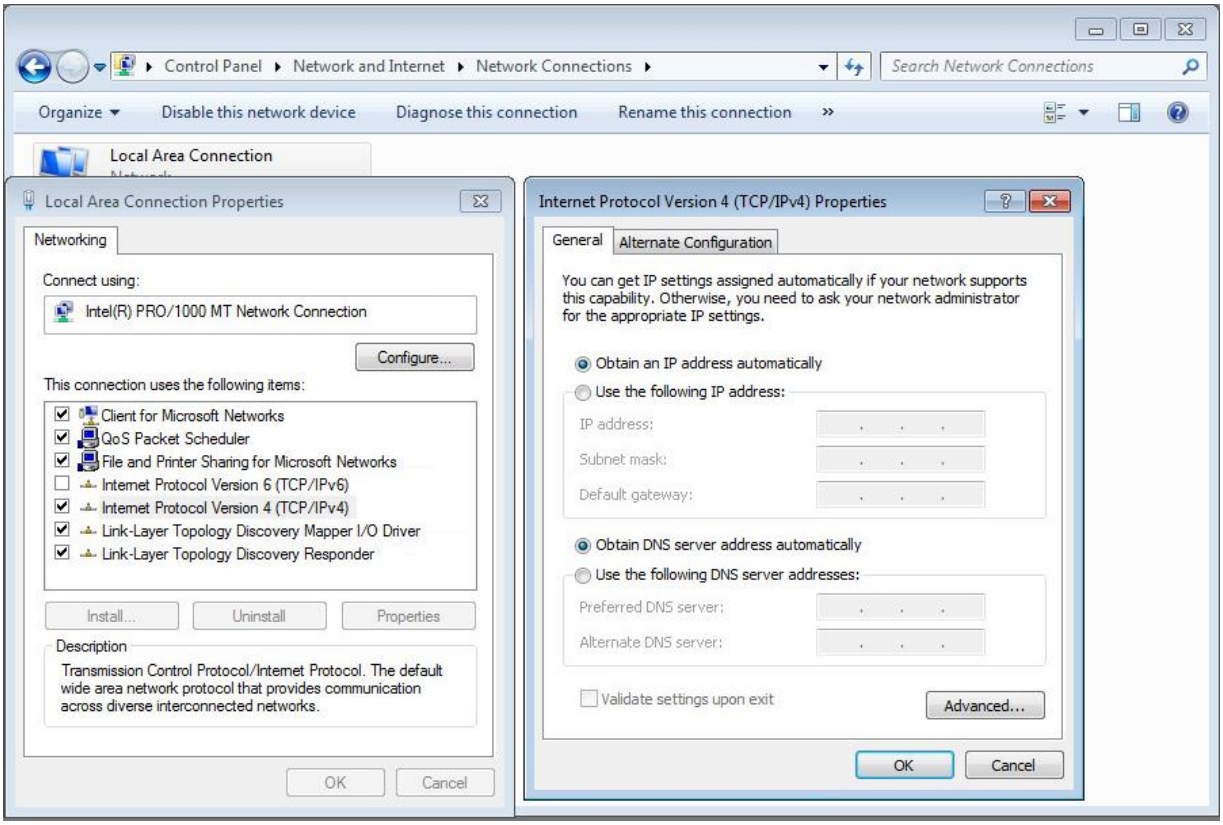
4. Установите время аренды в 8 часов (28800 минут).
   `ASA-X-1(config)# dhcpd lease 28800 interface inside`

5. Включите функционал DHCP-сервера на интерфейсе inside.
   `ASA-X-1(config)# dhcpd enable inside`
   `ASA-X-1(config)# exit`

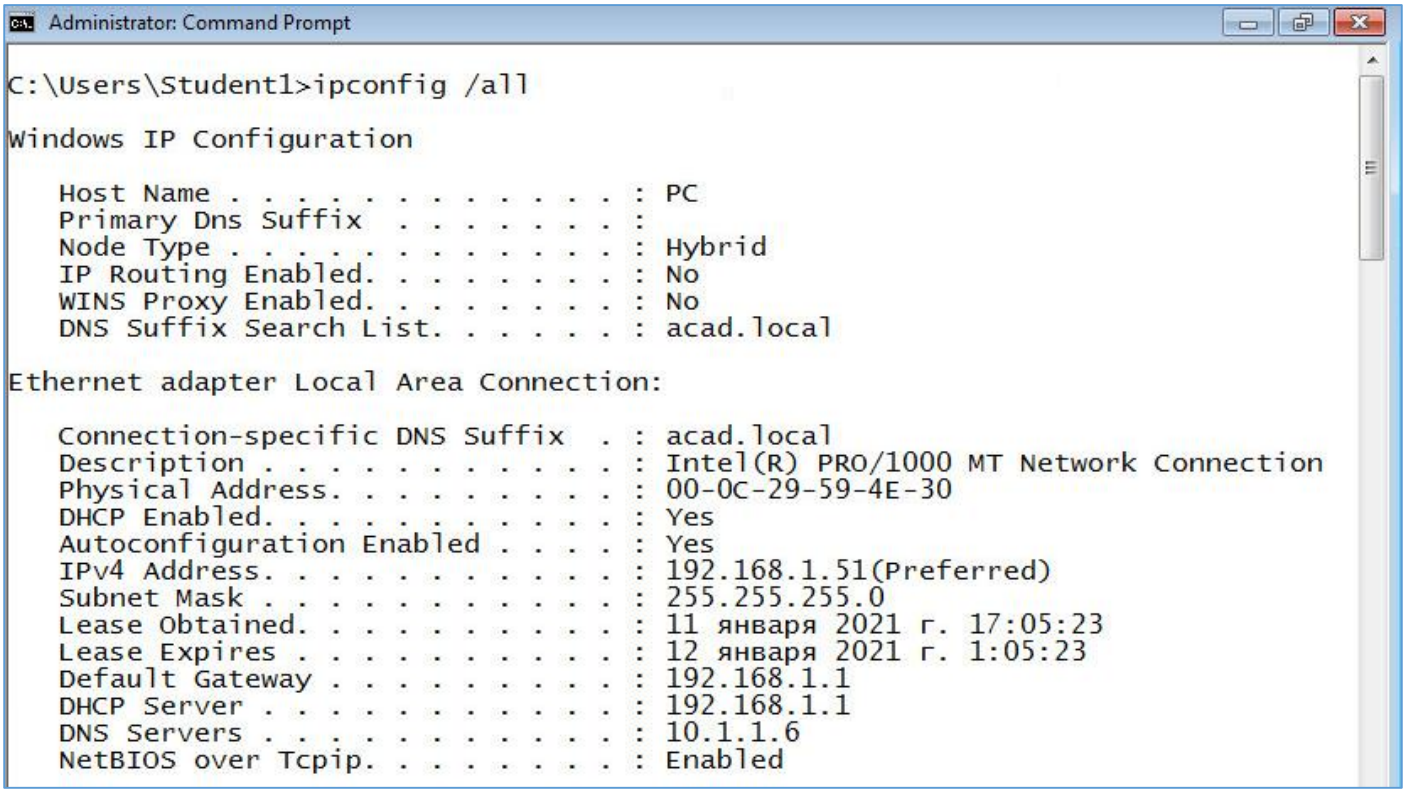
6. В качестве адреса шлюза ASA автоматически выдаст свой адрес на интерфейсе с именем inside.

7. Перейдите в виртуальную машину PC (PC-X-1 или PC-X-2).

8. Включите получение настроек по протоколу DHCP. Ниже представлен пример для левой части топологии.



9. Откройте командную строку и проверьте полученные настройки с помощью команды **ipconfig /all**.



10. Вернитесь в консоль ASA и посмотрите таблицу выданных адресов.

```
ASA-X-1# show dhcpd binding all
IP address        Client identifier Lease expiration        Type
```

```
192.168.1.51      0100.0c29.594e.30 28735 seconds           Automatic
```

Часть 8: Настройка сервисной политики

1. Cisco ASA использует многоуровневый подход при настройке правил фильтрации, похожий на ZPF,
   - классовые карты (class-map) определяют «интересный» траффик;
   - карты политик (policy-map) определяют действие с «интересным» траффиком;
   - сервисные политики (service-policy) определяют, когда вызывать карты политик.

   По умолчанию уже есть одна классовая карта, одна карта политик и одна глобальная сервисная политика. Глобальная сервисная политика срабатывает всегда.
   Посмотрите список созданных классовых карт.

```
ASA-X-1# show run class-map
!
class-map inspection_default
 match default-inspection-traffic
!
```

2. Посмотрите список созданных карт политик. Как видите, среди протоколов нет ICMP, следовательно, протокол ICMP не инспектируется.

```
ASA-X-1# show run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512

policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
```

3. Посмотрите список созданных сервисных политик.

```
ASA-X-1# show run service-policy
service-policy global_policy global
```

4. Любой движение траффика вызывает обращение к глобальной сервисной политике. Сервисная политика ссылается на карту политик global_policy. Карта политик global_policy ссылается на классовую карту inspection_default. Классовая карта inspection_default срабатывает, когда траффик относится к одному из протоколов (dns, ftp и т.д.). Включите инспекцию протокола ICMP.

```
ASA-X-1# conf t
ASA-X-1(config)# policy-map global_policy
ASA-X-1(config-pmap)# class inspection_default
ASA-X-1(config-pmap-c)# inspect icmp
ASA-X-1(config-pmap-c)# end
```

5. Посмотрите список созданных карт политик ещё раз.

```
ASA-X-1# show run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect icmp
!
```

6. Вернитесь в виртуальную машину PC (PC-X-1 или PC-X-2).

7. Откройте командную строку, проверьте связь со своим сервером PC-DMZ с помощью команды **ping**. Теперь проверка связи будет успешна. Почему?
   - Траффик поступил на интерфейс g0/0. Cisco ASA ищет, куда переслать пакет, согласно таблице маршрутов. Сеть получателя доступна как напрямую подключённая, найден выходной интерфейс g0/1;
   - Траффик идёт с интерфейса с уровнем безопасности 100 на интерфейс с уровнем безопасности 50, из большего уровня в меньший. Значит это исходящий траффик. Исходящий траффик разрешён, но пропускается через сервисную политику;

- Сервисная политика ссылается на карту политик global_policy. Карта политик global_policy ссылается на классовую карту inspection_default. Классовая карта inspection_default срабатывает, когда траффик относится к одному из протоколов, среди протоколов есть ICMP, значит классовая карта срабатывает. Карта политик инспектирует этот траффик: пакет разрешается, создаётся запись в таблице состояний, возвратный траффик будет автоматически разрешён.

8. Перейдите в виртуальную машину PC-DMZ (PC-DMZ-X-1 или PC-DMZ-X-2).

9. Откройте командную строку, проверьте связь с PC с помощью команды **ping**. Проверка связи будет неуспешна. Почему?
    - Траффик поступил на интерфейс g0/1. Cisco ASA ищет, куда переслать пакет, согласно таблице маршрутов. Сеть получателя доступна как напрямую подключённая, найден выходной интерфейс g0/0;
    - Траффик идёт с интерфейса с уровнем безопасности 50 на интерфейс с уровнем безопасности 100, из меньшего уровня в больший. Значит это входящий траффик. Входящий траффик по умолчанию запрещён, его надо явно разрешать с помощью списков контроля доступа.

10. Вернитесь в консоль ASA.

11. Сохраните конфигурацию.

```
ASA-X-1# copy run start

Source filename [running-config]? < Нажмите Enter >
Cryptochecksum: d0f4428c 9c6d3a00 db788aa3 b0963adc

7137 bytes copied in 0.210 secs
ASA-X-1#
```