

МДК.01.01

**Организация, принципы
построения и функционирования
компьютерных сетей
3-курс**

Практические занятия

Занятие 17



Тема: VPN соединение на Cisco ASA.

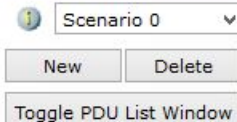
Рассмотрим построение **Site-to-Site VPN** на **Cisco ASA**.

К сожалению межсетевой экран в программе **Cisco** очень сильно урезан в функционале. Поэтому у нас не получится построить полноценную сеть, как это было с маршрутизаторами в предыдущей работе. Дело в том, что в этой версии программы невозможно организовать одновременную работу **NAT** и **VPN**.

В данном случае обойдёмся без технологии **NAT** и будем строить только **Site-to-Site VPN**.

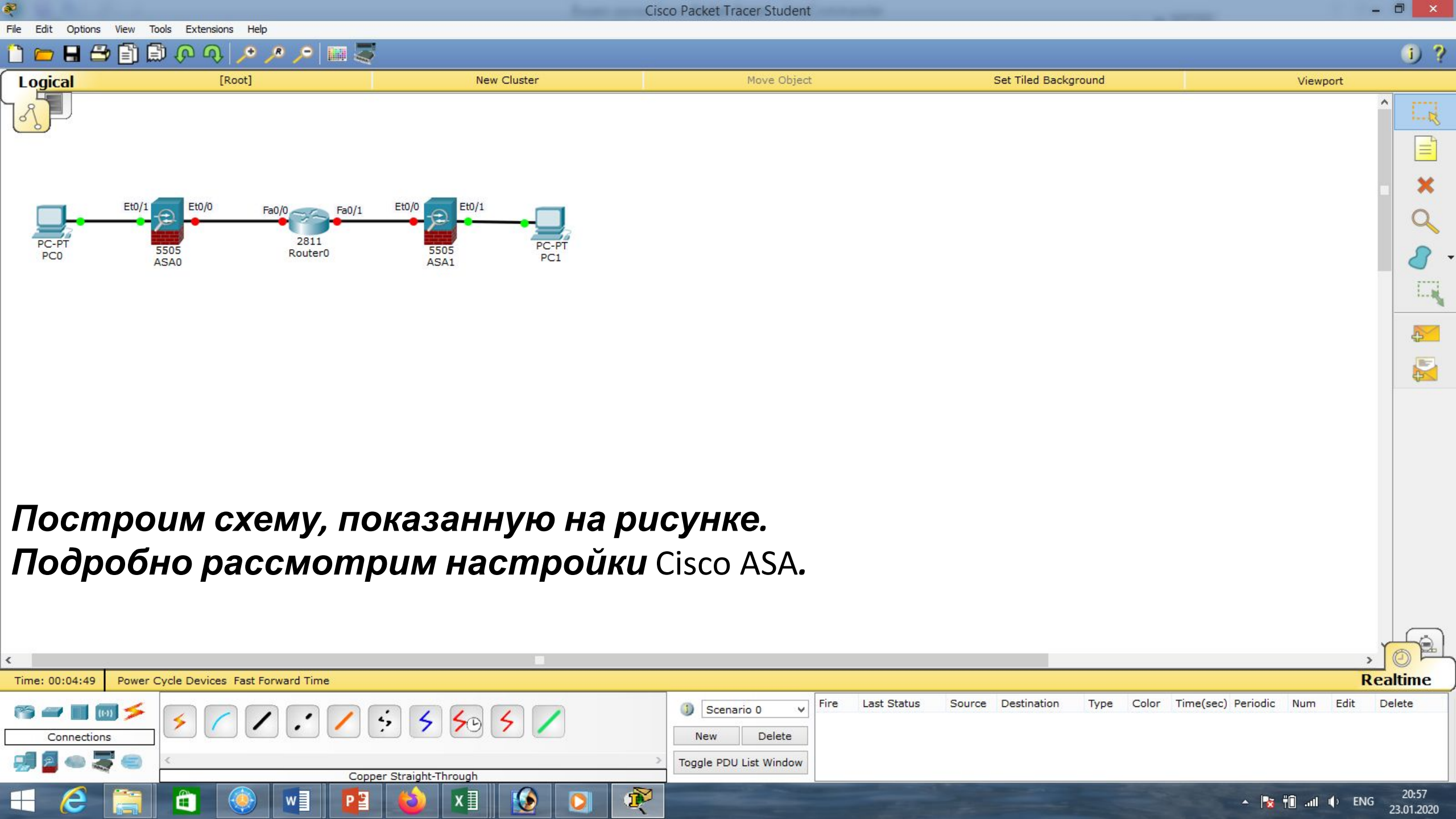


(Select a Device to Drag and Drop to the Workspace)



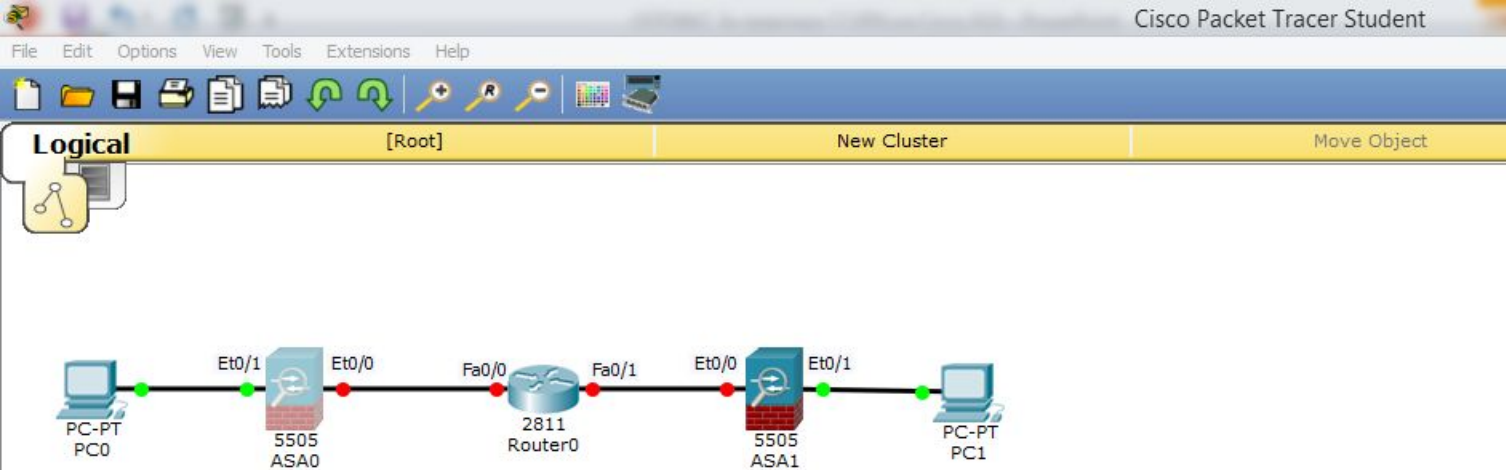
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------





**Построим схему, показанную на рисунке.
Подробно рассмотрим настройки Cisco ASA.**

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
[Empty table body]										



```
ASA0
Physical Config CLI
ASA Command Line Interface
-
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
```

Зайдём в настройки ASA0: «en», пароль пустой, поэтому просто нажимаем <Enter>, далее посмотрим заводские настройки: «show run», для продолжения просмотра нажимаем <Пробел>. Видим, что Ethernet0/0 уже настроен во vlan 2.

Time: 00:17:14 Power Cycle Devices Fast Forward Time Realtime

Scenario 0

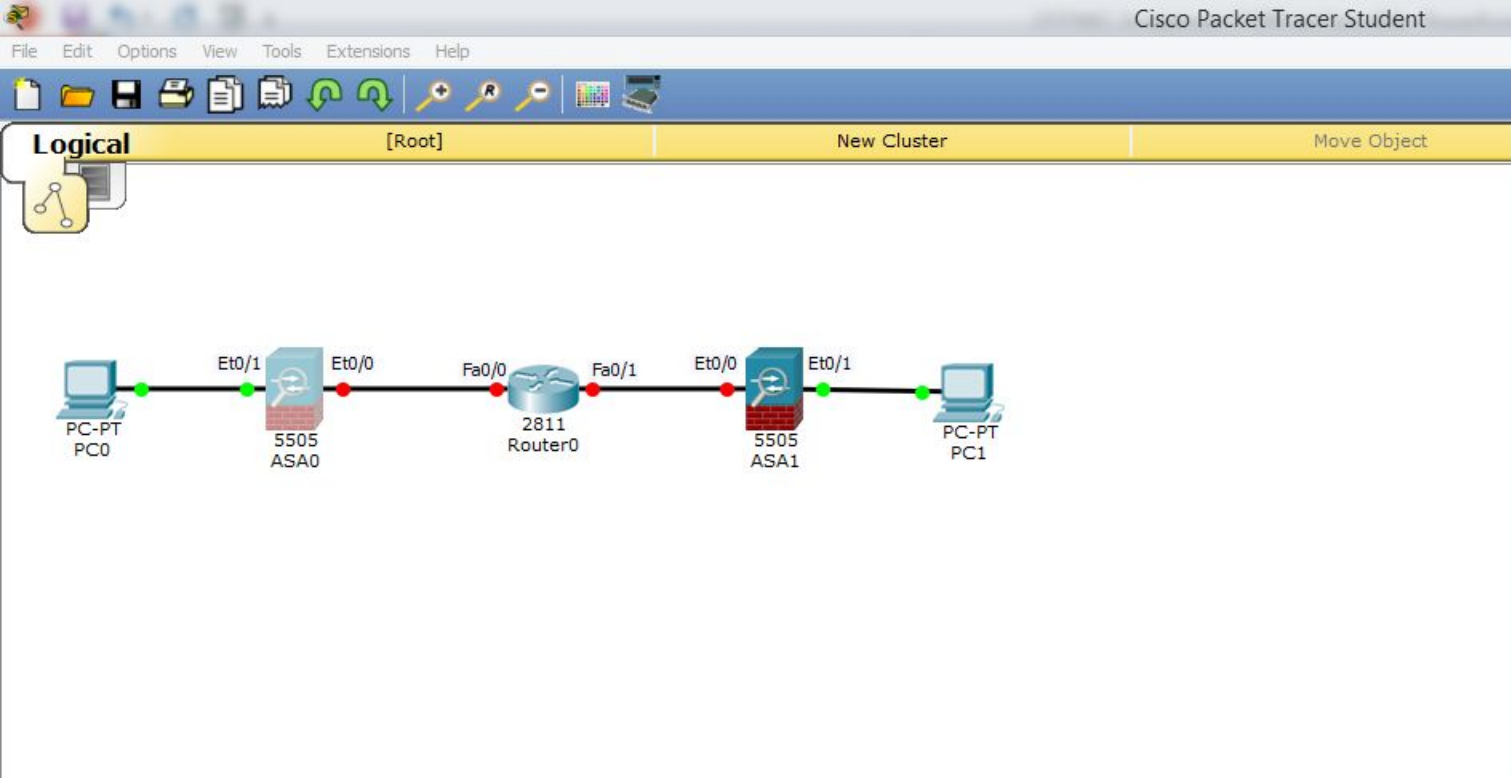
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Connections

Copper Straight-Through

Windows taskbar: Internet Explorer, File Explorer, Microsoft Store, Word, PowerPoint, Firefox, Excel, Chrome, VLC, Packet Tracer.

System tray: 21:09, 23.01.2020



```
ASA0
Physical Config CLI
ASA Command Line Interface
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp
!
!
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
```

Для продолжения просмотра нажимаем <Пробел>.
Видим, что interface Vlan2 является внешним интерфейсом (outside), ip-адрес ему не назначен. А interface Vlan1 является внутренним интерфейсом (inside) с уже назначенным шлюзом. Его ip-адрес: 192.168.1.1 255.255.255.0

Time: 00:22:00 | Power Cycle Devices | Fast Forward Time | Realtime

Scenario 0

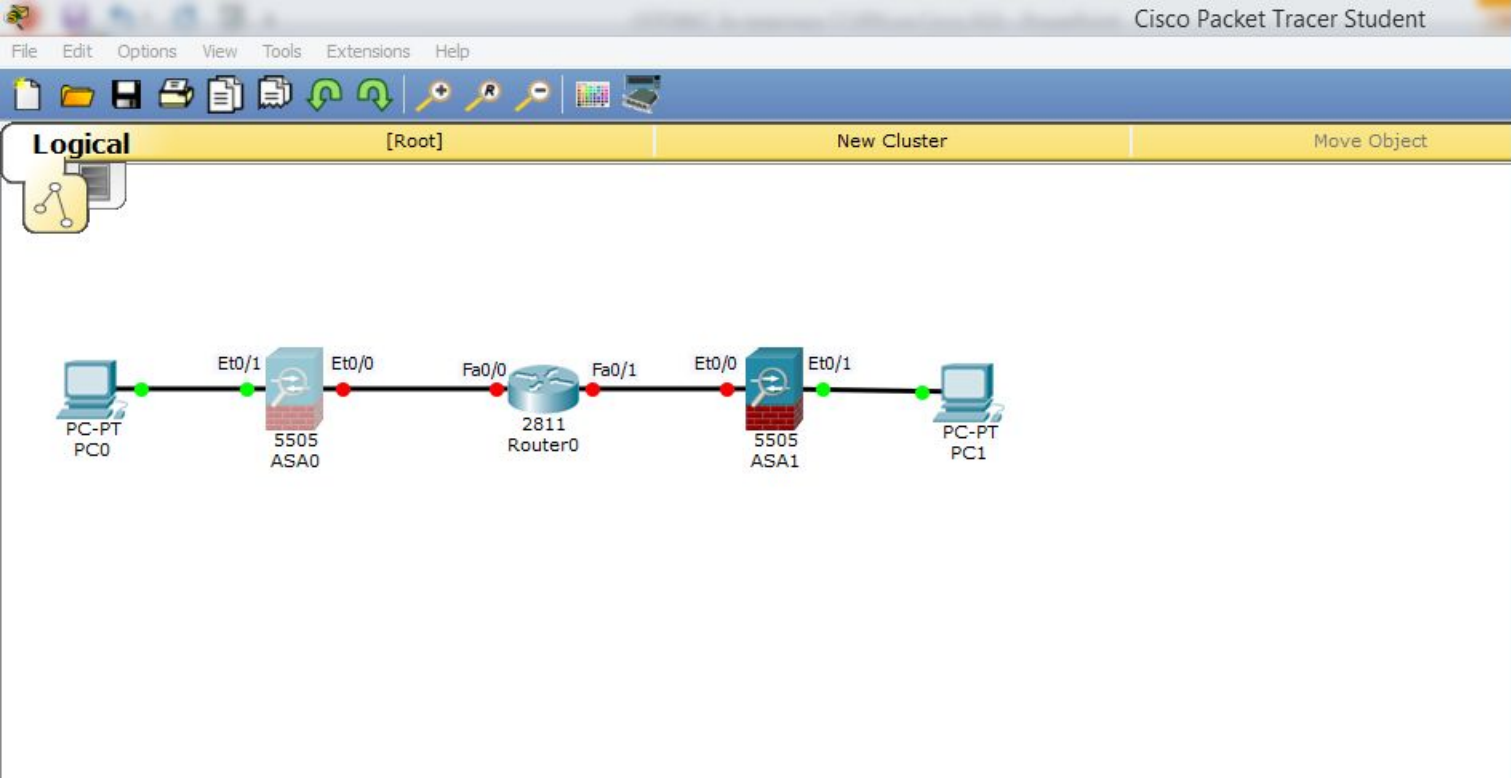
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Connections

Copper Straight-Through

Windows taskbar: File Explorer, Word, PowerPoint, Firefox, Excel, Chrome, VLC, Packet Tracer

System tray: 21:14, 23.01.2020



```
ASA0
Physical Config CLI
ASA Command Line Interface
!
!
!
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
dhcpd auto_config outside
!
!
!
!
!
!
ciscoasa#
```

Для продолжения просмотра нажимаем <Пробел>.
Видим, что на внутреннем интерфейсе уже настроен DHCP, при этом
указан диапазон ip-адресов: 192.168.1.5 - 192.168.1.35

Time: 00:31:13 Power Cycle Devices Fast Forward Time Realtime

Scenario 0

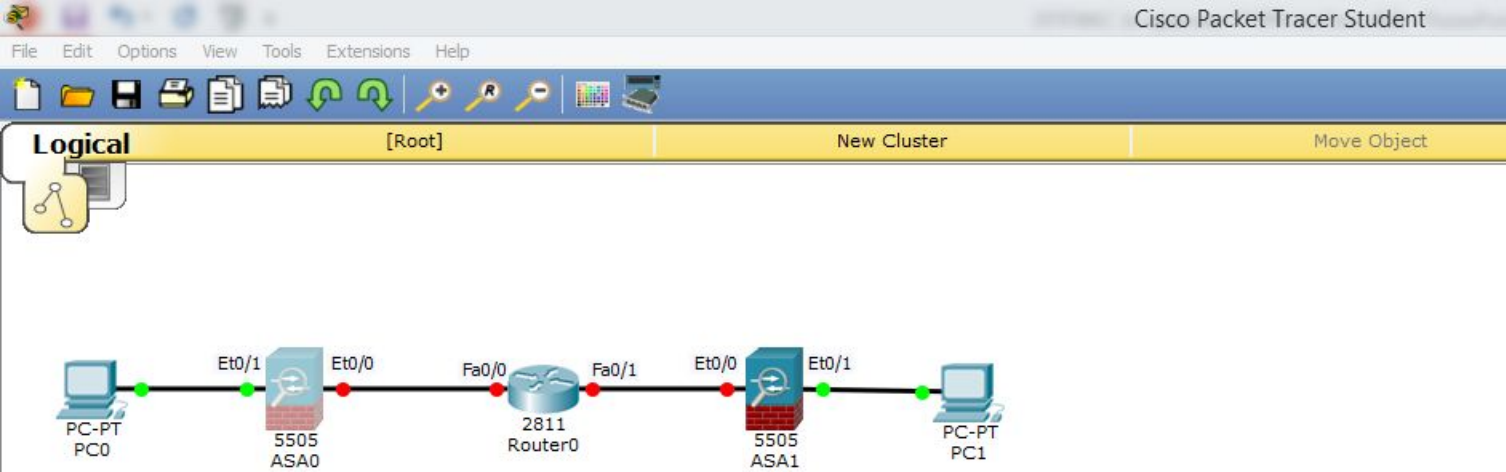
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Connections

Copper Straight-Through

Windows taskbar: Internet Explorer, File Explorer, Microsoft Store, Windows Defender, Word, PowerPoint, Firefox, Excel, Chrome, VLC, Packet Tracer.

System tray: ENG, 21:23, 23.01.2020



```
ASA0
Physical Config CLI
ASA Command Line Interface
!
!
!
!
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#int vl
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip add
ciscoasa(config-if)#ip address 210.210.1.2 255.255.255.252
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#ex
ciscoasa(config)#route ?

configure mode commands/options:
  inside  Name of interface Vlan1
  outside Name of interface Vlan2
ciscoasa(config)#route out
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 210.210.1.1
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
```

Зададим маршрут по умолчанию на внешний интерфейс через ip-адрес интернет-провайдера (210.210.1.1): «conf t», «route outside 0.0.0.0 0.0.0.0 210.210.1.1».

Time: 00:53:12 Power Cycle Devices Fast Forward Time Realtime

Connections

Copper Straight-Through

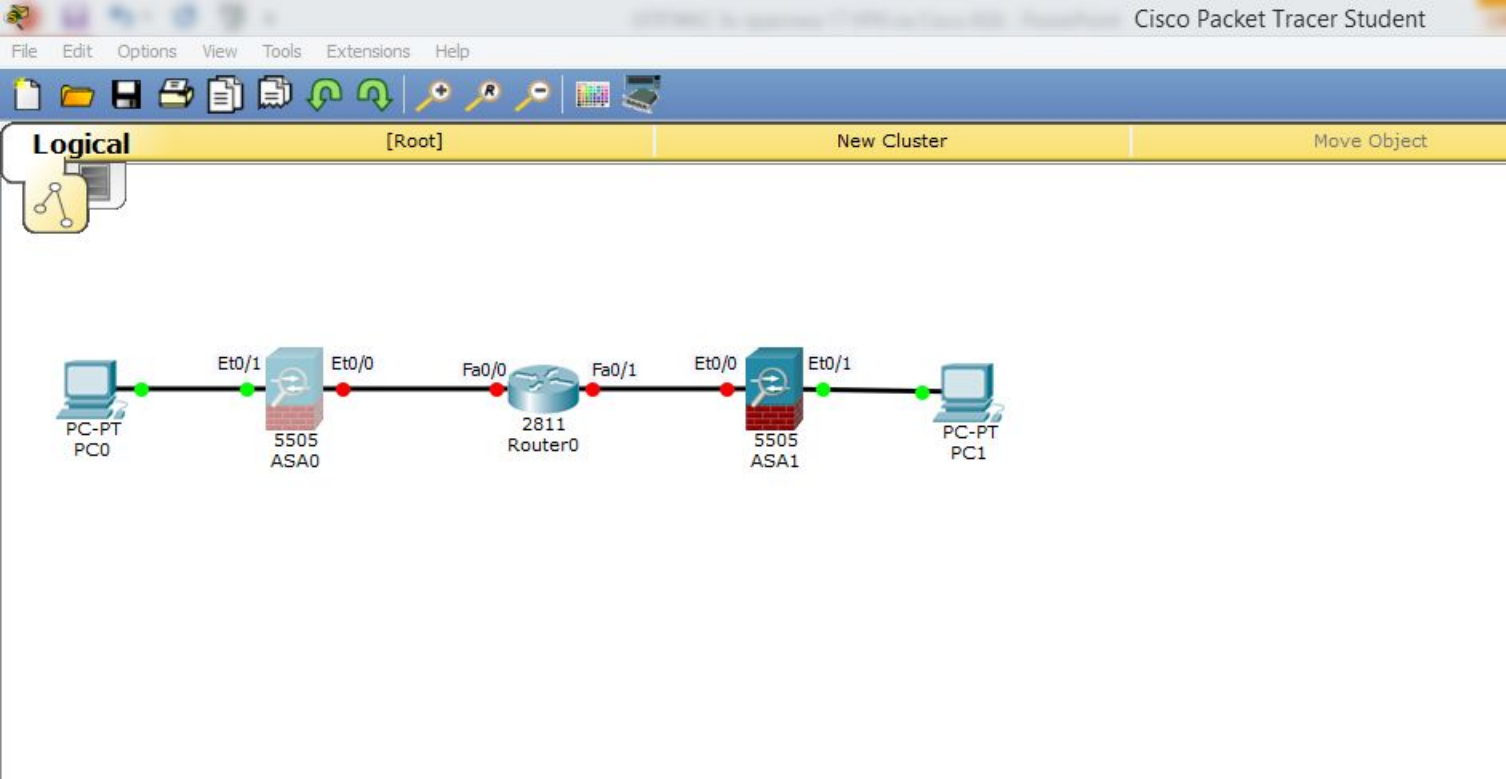
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Scenario 0

New Delete

Toggle PDU List Window

Windows taskbar: 21:46 23.01.2020



```
ASA0
Physical Config CLI
ASA Command Line Interface
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
```

Далее создаём политику (действие над трафиком):
«policy-map global_policy».
Это действие применяется к созданному нами классу: «class inspection_default», **нас интересует инспектирование трафика icmp:** «inspect icmp» «exit».

Time: 01:19:47 | Power Cycle Devices | Fast Forward Time | Realtime

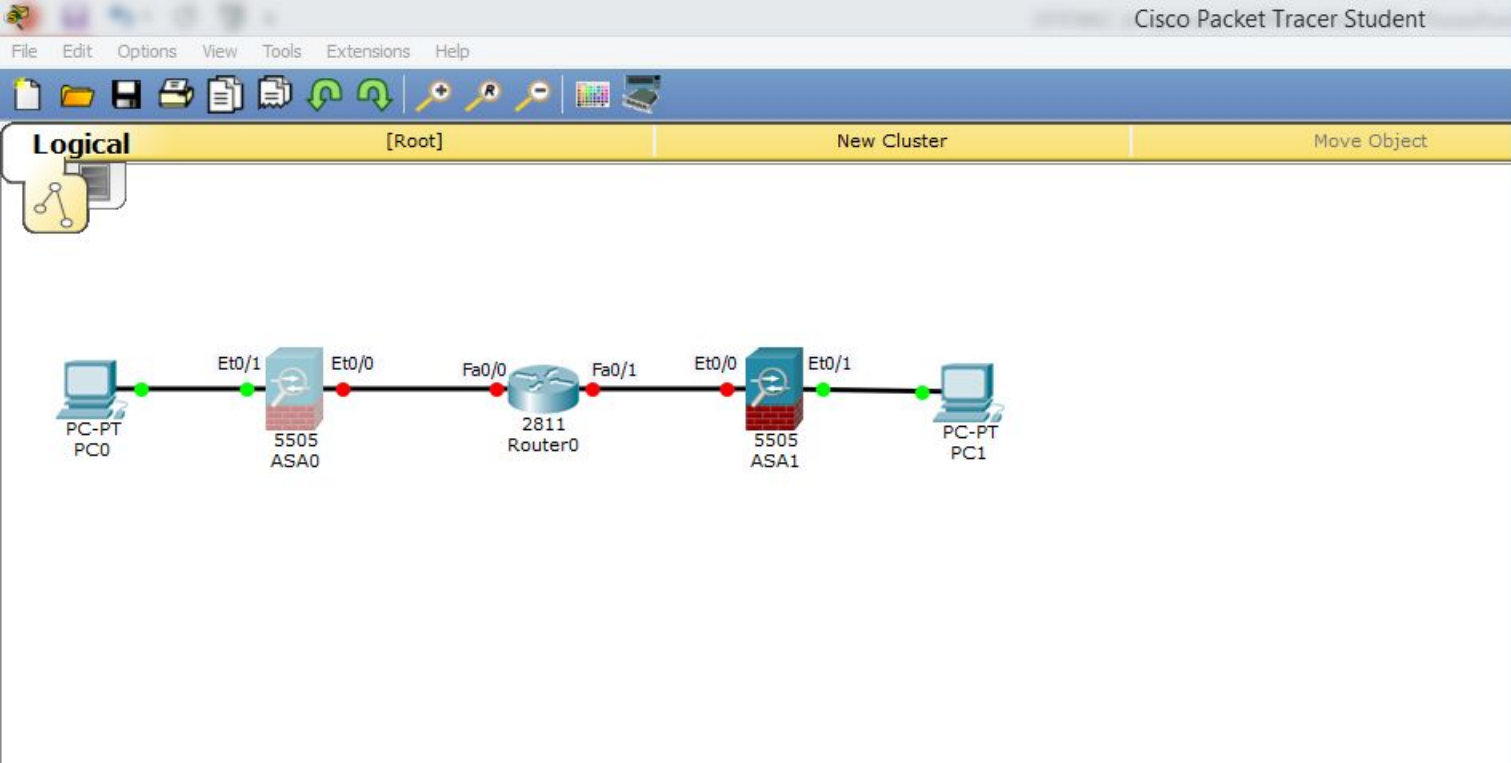
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Scenario 0 | New | Delete | Toggle PDU List Window

Connections | Copper Straight-Through

Windows taskbar: File Explorer, Word, Firefox, Excel, PowerPoint, etc.

System tray: 22:12, 23.01.2020



```
ASA0
Physical Config CLI
ASA Command Line Interface
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#service-policy global_policy global
ciscoasa(config)#end
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 3c8246d4 3f837647 3f331ad0 1dc13e50

938 bytes copied in 1.311 secs (715 bytes/sec)
[OK]
ciscoasa#
```

Далее определяем, в каком направлении будем использовать политику инспектирования трафика. В нашем случае во всех направлениях:
«service-policy global_policy global»,
«end»,
«wr mem».

Time: 01:24:43 Power Cycle Devices Fast Forward Time Realtime

Connections

Copper Straight-Through

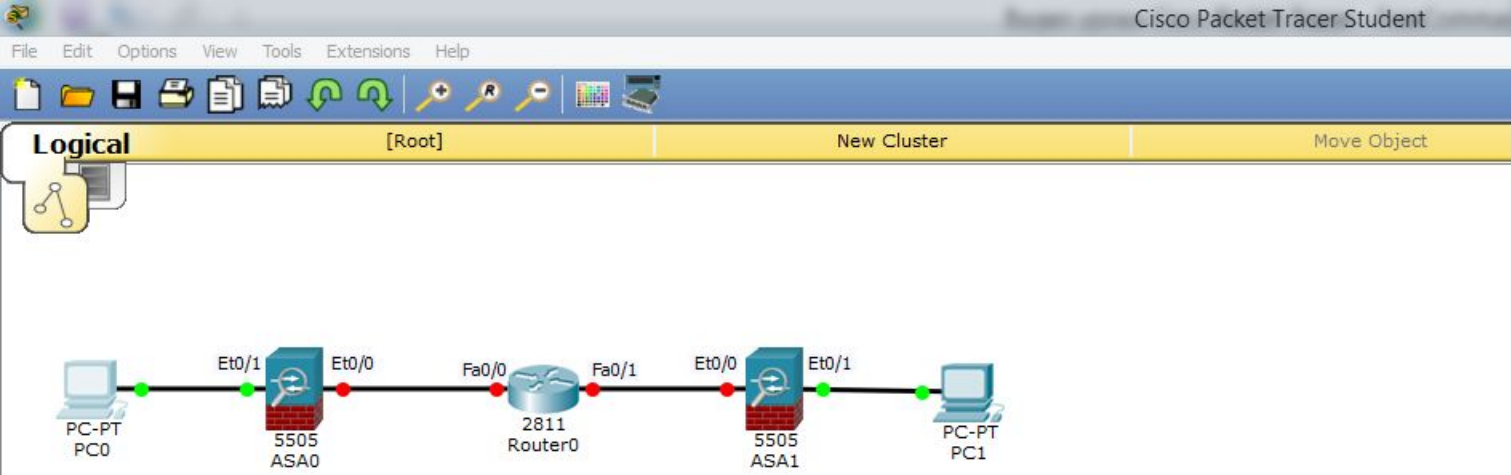
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Scenario 0

New Delete

Toggle PDU List Window

Windows taskbar: 22:17 23.01.2020



PCO

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

DHCP Static DHCP request successful.

IP Address: 192.168.1.5

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server:

IPv6 Configuration

DHCP Auto Config Static

IPv6 Address:

Link Local Address: FE80::204:9AFF:FEC7:BCE6

IPv6 Gateway:

IPv6 DNS Server:

Так как DHCP на Cisco ASA уже настроен, зайдём в настройки компьютера, выбираем DHCP, видим, что нам выдали первый ip-адрес из всего диапазона ip-адресов (192.168.1.5).

Time: 00:44:43 Power Cycle Devices Fast Forward Time

Connections

Copper Straight-Through

Scenario 0

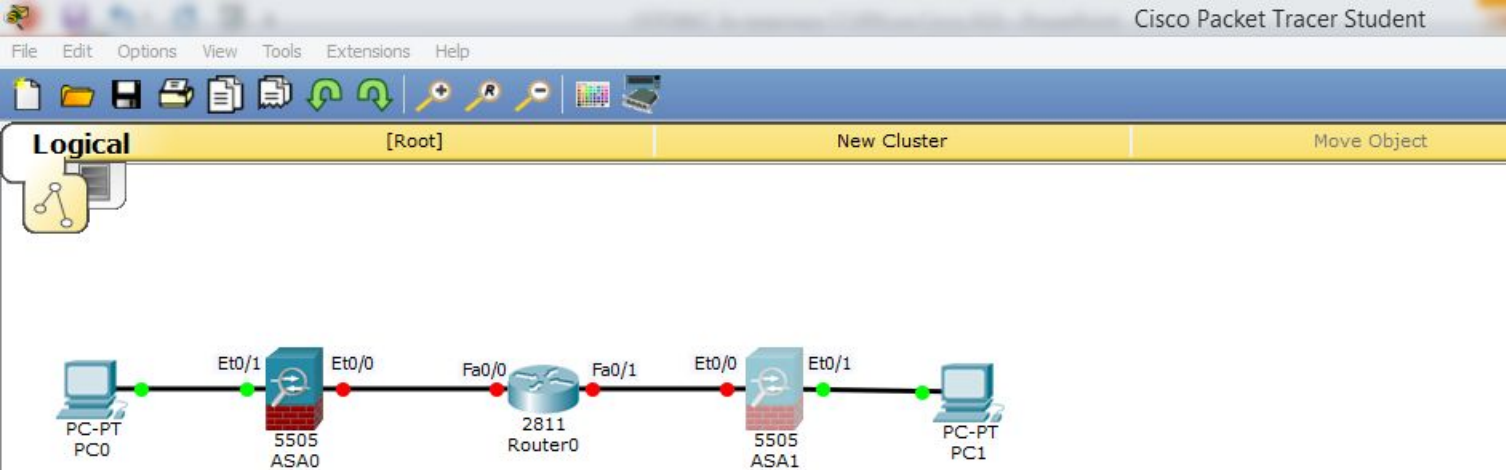
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

New Delete

Toggle PDU List Window

Realtime

21:37 23.01.2020



```
ASA1
Physical Config CLI
ASA Command Line Interface
!
!
!
!
ciscoasa#conf t
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside
ciscoasa(config)#
ciscoasa(config)#interface Vlan1
ciscoasa(config-if)#
ciscoasa(config-if)#ip add
ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0
ciscoasa(config-if)#
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#dhcpd address 192.168.2.5-192.168.2.35 inside
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
```

Для этого удалим pool ip-адресов DHCP **и исправим** ip-адрес **на внутреннем интерфейсе** (vlan 1): «conf t», «no dhcpd address 192.168.1.5-192.168.1.35 inside», «interface Vlan1», «ip address 192.168.2.1 255.255.255.0», «no shutdown». **Добавим новый** pool: «dhcpd address 192.168.2.5-192.168.2.35 inside».

Time: 01:53:04 Power Cycle Devices Fast Forward Time Realtime

Scenario 0

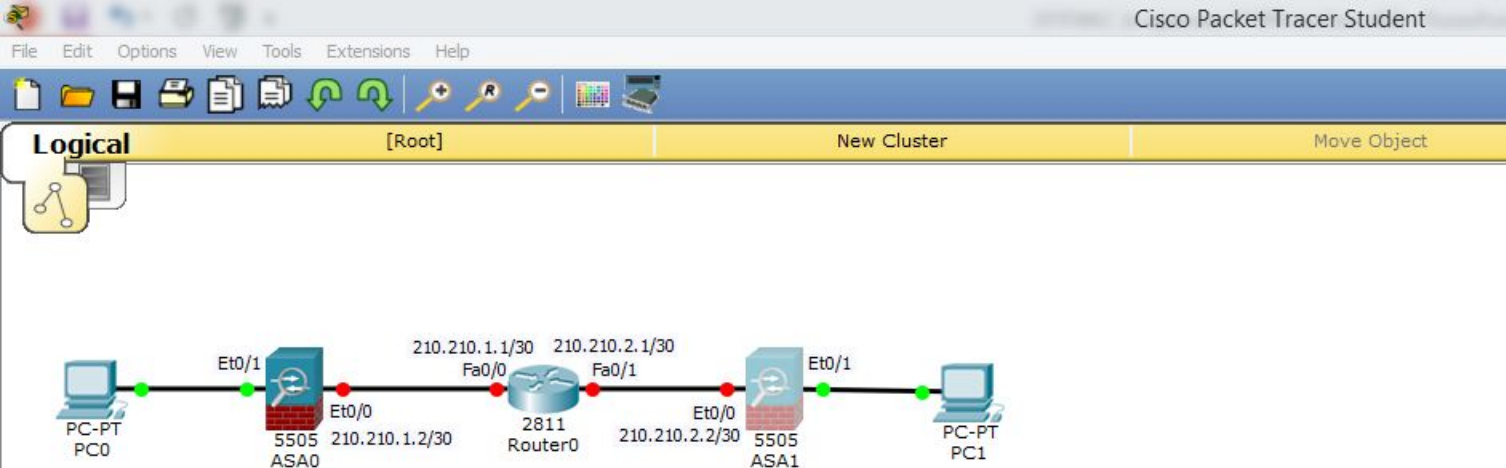
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Connections

Copper Straight-Through

Windows taskbar: Internet Explorer, File Explorer, Word, Firefox, Excel, PowerPoint, VLC, Packet Tracer

System tray: ENG, 22:46, 23.01.2020



```
ASA1
Physical Config CLI
ASA Command Line Interface
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside
ciscoasa(config)#
ciscoasa(config)#interface Vlan1
ciscoasa(config-if)#
ciscoasa(config-if)#ip add
ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0
ciscoasa(config-if)#
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#dhcpd address 192.168.2.5-192.168.2.35 inside
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip address 210.210.2.2 255.255.255.252
ciscoasa(config-if)# no sh
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)#
ciscoasa(config-if)#
```

Заддим ip-адрес **на внешнем интерфейсе** (vlan 2):
«int vlan 2»,
«ip address 210.210.2.2 255.255.255.252»,
«no shutdown».

Time: 02:09:10 Power Cycle Devices Fast Forward Time **Realtime**

Scenario 0

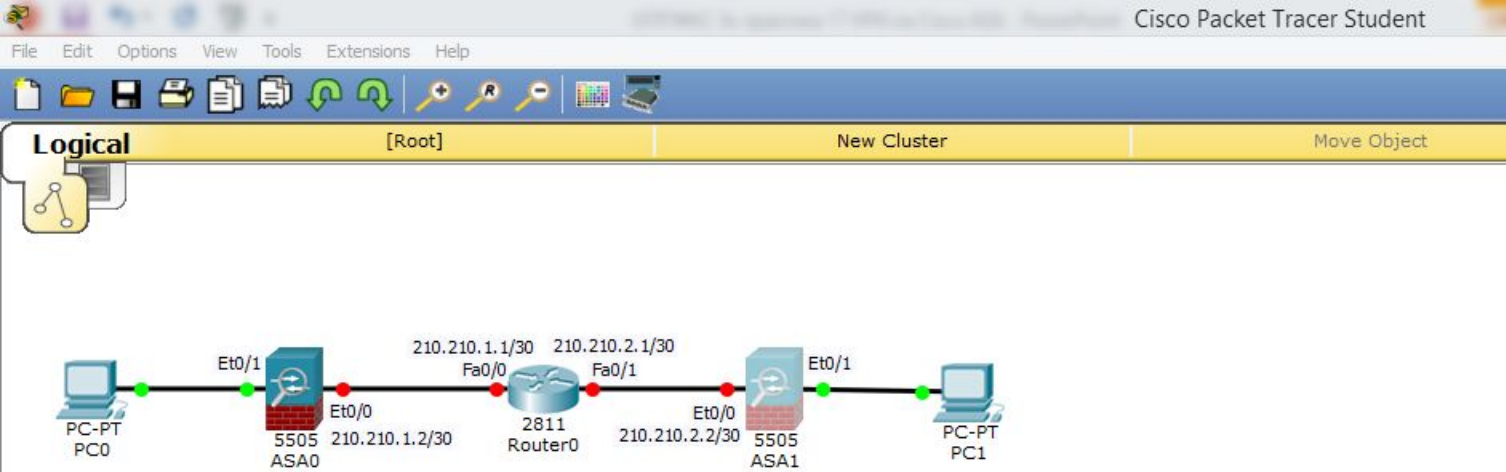
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Connections

Copper Straight-Through

Windows taskbar: Internet Explorer, File Explorer, Microsoft Store, Word, Firefox, Excel, Chrome, PowerPoint, VLC, Task Manager

System tray: ENG, 23:02, 23.01.2020



```
ASA1
Physical Config CLI
ASA Command Line Interface
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside
ciscoasa(config)#
ciscoasa(config)#interface Vlan1
ciscoasa(config-if)#
ciscoasa(config-if)#ip add
ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0
ciscoasa(config-if)#
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#dhcpd address 192.168.2.5-192.168.2.35 inside
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip address 210.210.2.2 255.255.255.252
ciscoasa(config-if)# no sh
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)#
ciscoasa(config-if)#route outside 0.0.0.0 0.0.0.0 210.210.2.1
ciscoasa(config)#
```

Зададим маршрут по умолчанию на внешний интерфейс через ip-адрес интернет-провайдера (210.210.2.1):
«conf t»,
«route outside 0.0.0.0 0.0.0.0 210.210.2.1».

Time: 02:12:06 Power Cycle Devices Fast Forward Time **Realtime**

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

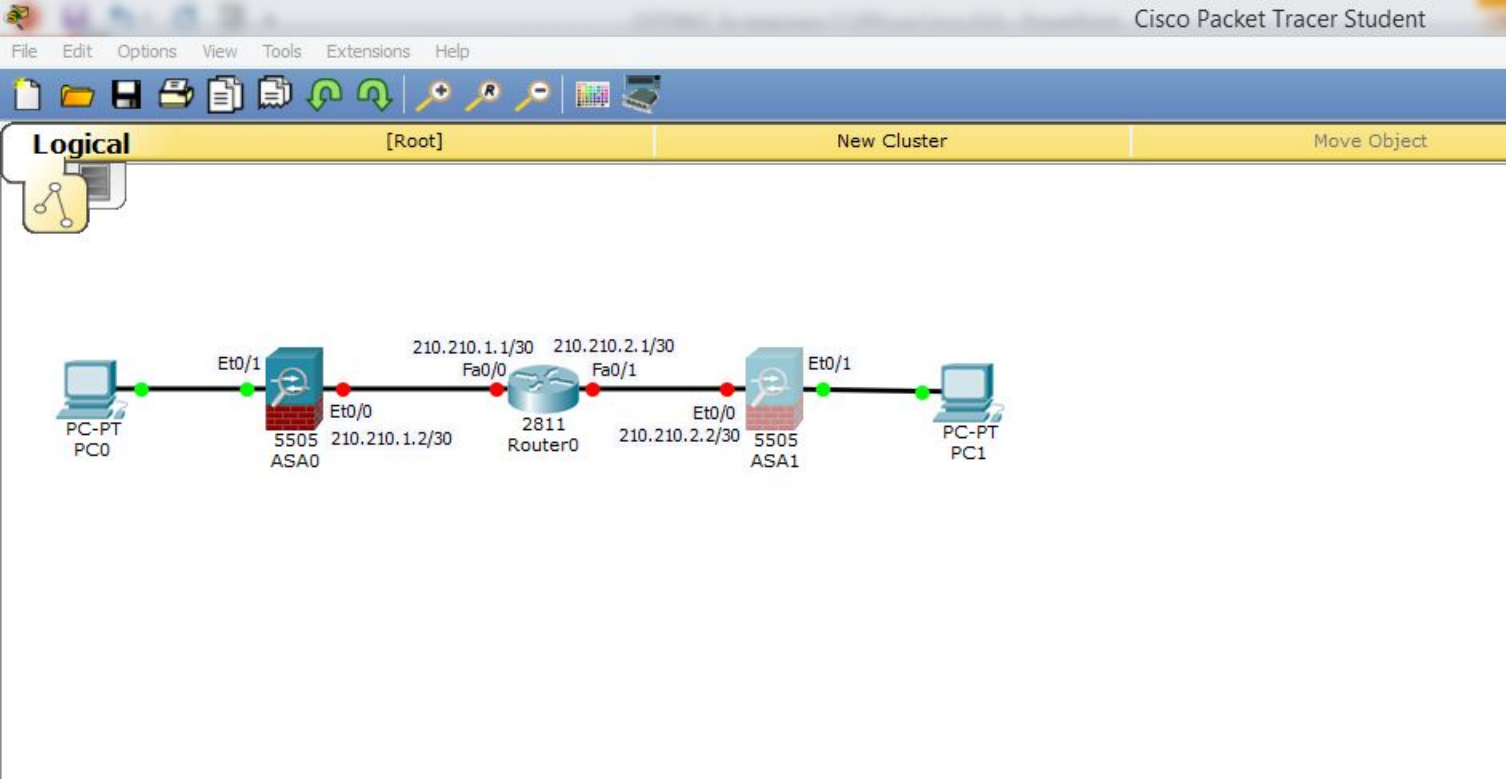
Connections

Copper Straight-Through

New Delete

Toggle PDU List Window

Windows taskbar: 23:05 23.01.2020



```
ASA1
Physical Config CLI
ASA Command Line Interface
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#dhcpd address 192.168.2.5-192.168.2.35 inside
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip address 210.210.2.2 255.255.255.252
ciscoasa(config-if)#no sh
ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#
ciscoasa(config-if)#route outside 0.0.0.0 0.0.0.0 210.210.2.1
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#
ciscoasa(config-cmap)#exit
ciscoasa(config)#
ciscoasa(config)#
```

Далее нужно настроить инспектирование трафика. Сначала определяем тип трафика, который хотим инспектировать: «class-map inspection_default», указываем весь трафик: «match default-inspection-traffic», «exit».

Time: 02:16:14 Power Cycle Devices Fast Forward Time **Realtime**

Scenario 0

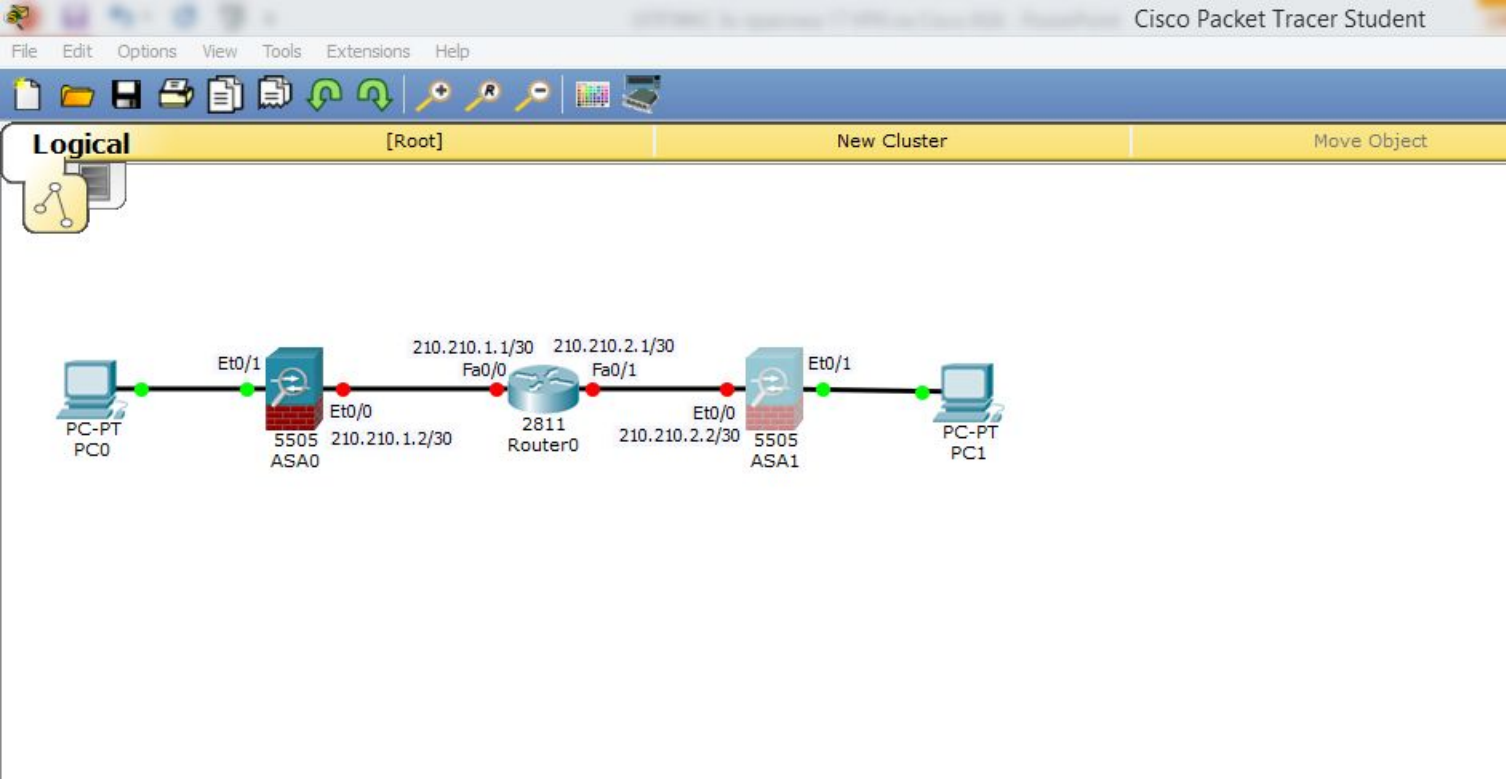
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Connections

Copper Straight-Through

Windows taskbar: Internet Explorer, File Explorer, Microsoft Word, Firefox, Microsoft Excel, Google Chrome, PowerPoint, VLC Media Player.

System tray: ENG, 23:09, 23.01.2020



```

ASA1
Physical Config CLI
ASA Command Line Interface
ciscoasa(config-if)# ip address 210.210.2.2 255.255.255.252
ciscoasa(config-if)# no sh
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)#
ciscoasa(config-if)#route outside 0.0.0.0 0.0.0.0 210.210.2.1
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#
ciscoasa(config-cmap)#exit
ciscoasa(config)#
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#
ciscoasa(config)#
  
```

Далее создаём политику (действие над трафиком):
 «policy-map global_policy».
Это действие применяется к созданному нами классу: «class inspection_default», **нас интересует инспектирование трафика icmp:** «inspect icmp», «exit».

Time: 02:20:41 | Power Cycle Devices | Fast Forward Time | Realtime

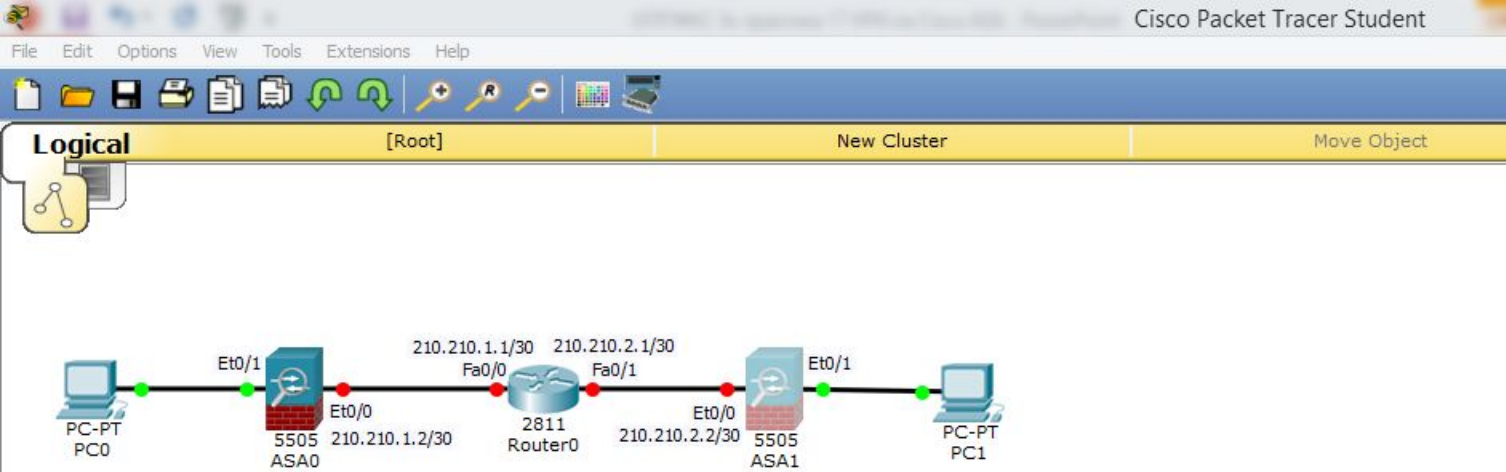
Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete

Connections: Copper Straight-Through

Windows taskbar: File Explorer, Word, Firefox, Excel, PowerPoint, etc.

System tray: 23:13, 23.01.2020



```
ASA1
Physical Config CLI
ASA Command Line Interface
ciscoasa(config-cmap)#
ciscoasa(config-cmap)#exit
ciscoasa(config)#
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#
ciscoasa(config)#service-policy global_policy global
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 26000853 07a73a53 6ee76e33 1b801986

938 bytes copied in 1.45 secs (646 bytes/sec)
[OK]
ciscoasa#
ciscoasa#
ciscoasa#
```

Далее определяем, в каком направлении будем использовать политику инспектирования трафика. В нашем случае во всех направлениях:
«service-policy global_policy global»,
«end»,
«wr mem».

Time: 02:23:30 Power Cycle Devices Fast Forward Time Realtime

Scenario 0

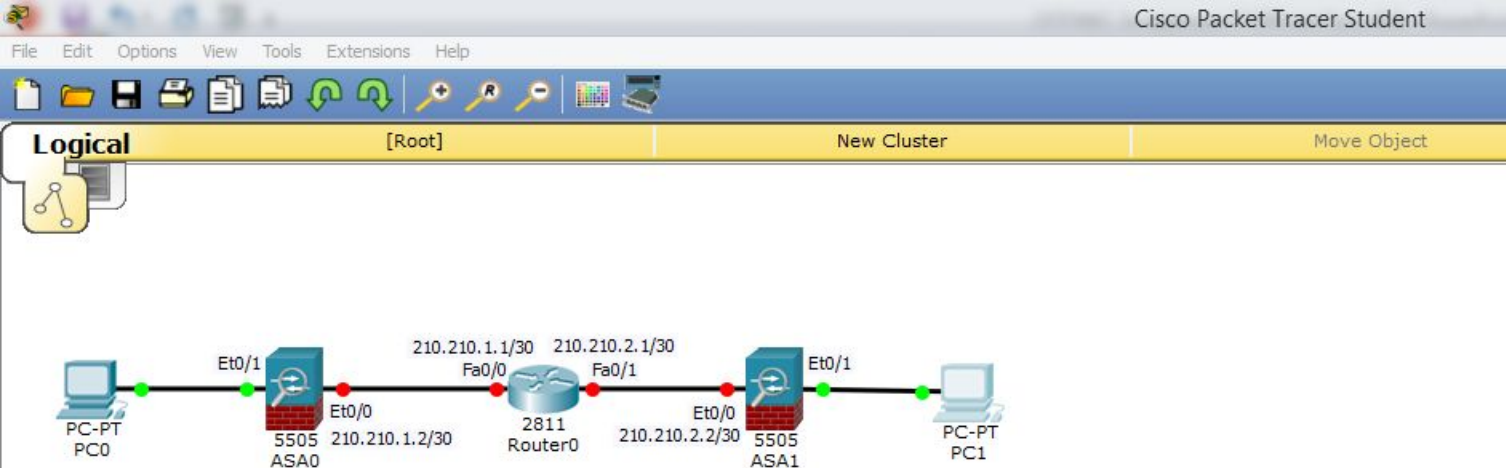
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Connections

Copper Straight-Through

Windows taskbar: Internet Explorer, File Explorer, Microsoft Word, Firefox, Microsoft Excel, Google Chrome, PowerPoint, VLC Media Player.

System tray: 23:16, 23.01.2020, ENG



PC1

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

DHCP Static DHCP request successful.

IP Address: 192.168.2.5

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server:

IPv6 Configuration

DHCP Auto Config Static

IPv6 Address: /

Link Local Address: FE80::209:7CFF:FED7:2620

IPv6 Gateway:

IPv6 DNS Server:

Так как DHCP на Cisco ASA уже настроен, зайдём в настройки компьютера, выбираем DHCP, видим, что нам выдали первый ip-адрес из нового диапазона ip-адресов, который мы создали (192.168.2.5).

Time: 02:24:50 Power Cycle Devices Fast Forward Time

Connections

Copper Straight-Through

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

New Delete

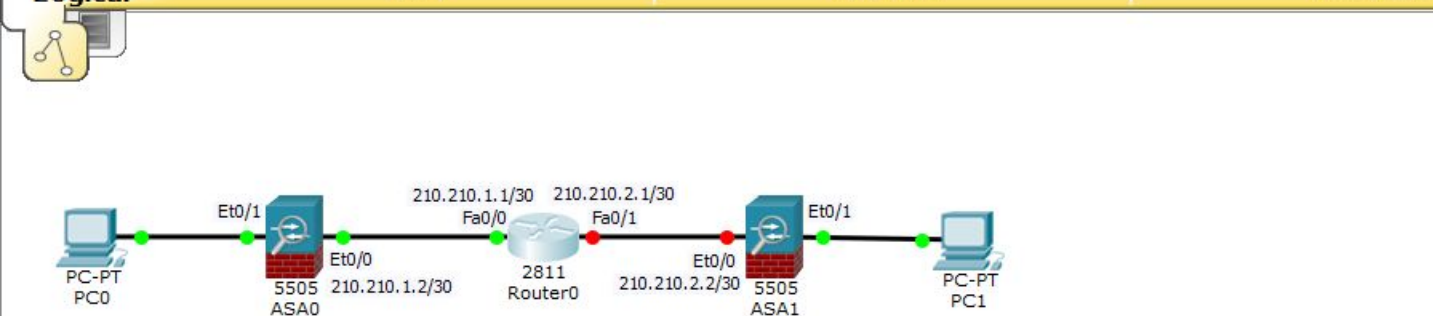
Toggle PDU List Window

Realtime

23:17 23.01.2020



Logical [Root] New Cluster Move Object



Настроим ip-адреса на маршрутизаторе интернет-провайдера (Router0):

«n»,

«en»,

«conf t»,

«int fa0/0»,

«ip address 210.210.1.1 255.255.255.252»,

«no shutdown»,

«exit».

Router0

Physical Config CLI

IOS Command Line Interface

```
Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add
Router(config-if)#ip address 210.210.1.1 255.255.255.252
Router(config-if)#no sh
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

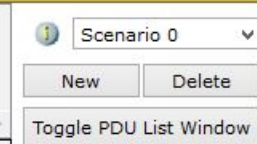
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#
```

Copy Paste

Time: 02:33:19 Power Cycle Devices Fast Forward Time

Realtime

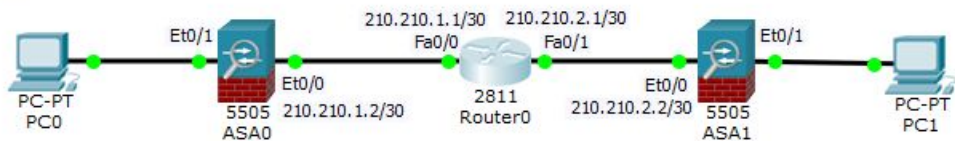


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------





Logical [Root] New Cluster Move Object

**Далее:**

«int fa0/1»,

«ip address 210.210.2.1 255.255.255.252»,

«no shutdown»,

«end»,

«wr mem».

Router0

Physical Config CLI

IOS Command Line Interface

```
Router(config)#
Router(config)#
Router(config)#int fa0/1
Router(config-if)#
Router(config-if)#ip address 210.210.2.1 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

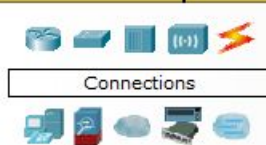
Router(config-if)#exit
Router(config)#e
% Ambiguous command: "e"
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
Router#
```

Copy Paste

Time: 02:42:53 Power Cycle Devices Fast Forward Time

Realtime



Copper Straight-Through

Scenario 0

New Delete

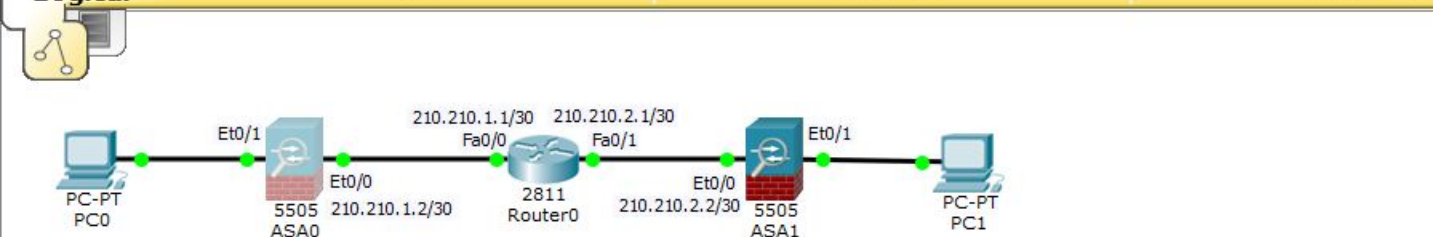
Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------





Logical [Root] New Cluster Move Object



ASA0

Physical Config CLI

ASA Command Line Interface

```
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#ping 210.210.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.210.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
```

Copy Paste

Проверим связь между межсетевыми экранами:

«ping 210.210.2.2».

Связь есть!!!

Далее нужно бы настроить NAT, но так как он не работает совместно с VPN, то приступим к настройке VPN. На реальном оборудовании такого ограничения быть не должно. Возможно, его не будет в следующей версии программы. Делается это также как в предыдущей работе, кроме некоторых команд.

Time: 02:48:12 Power Cycle Devices Fast Forward Time

Realtime



Copper Straight-Through

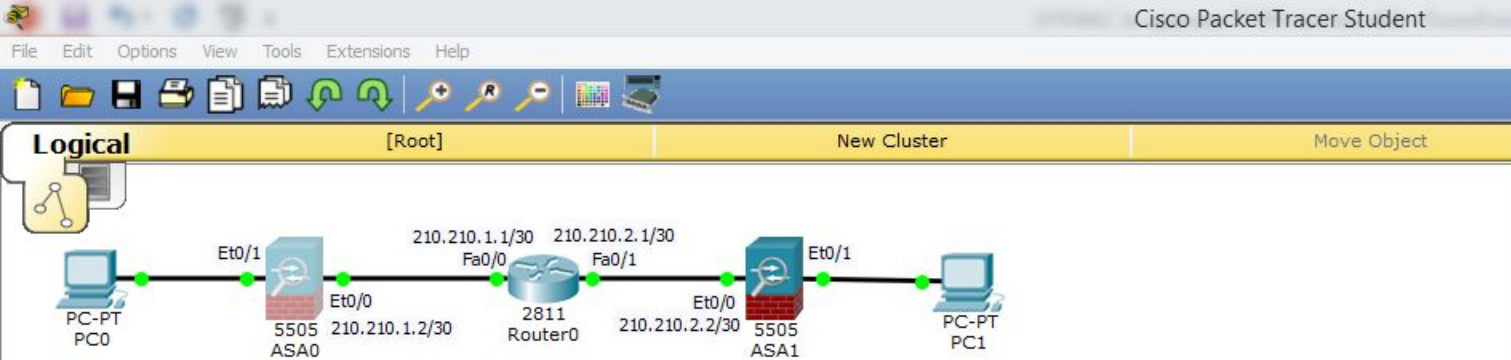
Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------





```
ASA0
Physical Config CLI
ASA Command Line Interface
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#cry
ciscoasa(config)#crypto ik
ciscoasa(config)#crypto ikev1 ena
ciscoasa(config)#crypto ikev1 enable out
ciscoasa(config)#crypto ikev1 enable outside
ciscoasa(config)#
ciscoasa(config)#crypto ikev1 pol
ciscoasa(config)#crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)#enc
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash md5
ciscoasa(config-ikev1-policy)#aut
ciscoasa(config-ikev1-policy)#authentication pre
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#g
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#exit
ciscoasa(config)#
ciscoasa(config)#
```

Начнём с маршрутизатора центрального офиса Router0. **Для начала нам необходимо настроить** первую фазу. **На внешнем интерфейсе включим протокол ike:** «crypto ikev1 enable outside» **Далее создаётся политика:** «crypto ikev1 policy 1» **где мы указываем алгоритм шифрования 3des (это параметры для построения мини туннеля ISAKMP-туннеля, через который будут передаваться параметры основного Ipsec-туннеля):** «encryption 3des», **алгоритм хеширования md5:** «hash md5», **тип аутентификации Pre-Shared Key:** «authentication pre-share» **и алгоритм Диффи – Хеллмана:** «group 2», «exit»

Power Cycle Devices Fast Forward Time Realtime

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

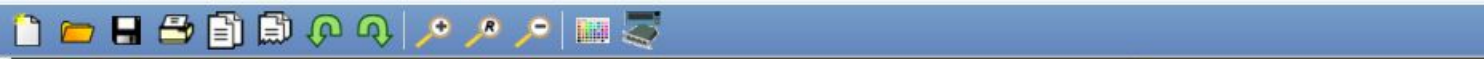
Scenario 0

New Delete

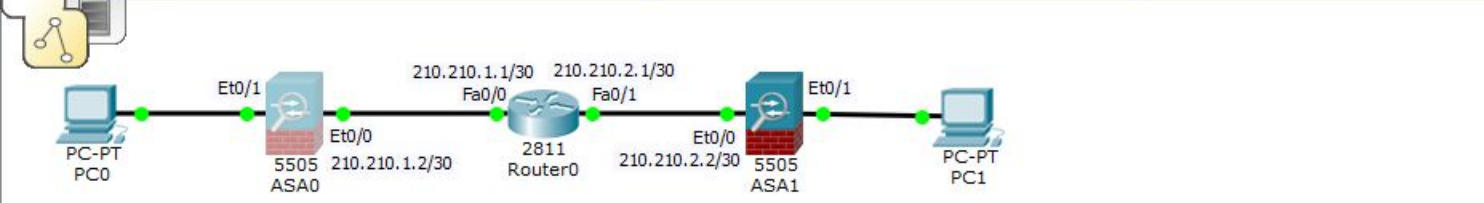
Toggle PDU List Window

Copper Straight-Through

0:05 24.01.2020



Logical [Root] New Cluster Move Object



Настроим ключ аутентификации и адреса пира, то есть внешнего ip-адреса межсетевого экрана

ASA1, с которым будем строить VPN:

«tunnel-group 210.210.2.2 type ipsec-l2l».

Зададим атрибуты ipsec:

«tunnel-group 210.210.2.2 ipsec-attributes»,

«ikev1 pre-shared-key cisco», «exit».

Мы настроили параметры, необходимые для первой фазы.

Переходим ко второй фазе.

ASA0

Physical Config CLI

ASA Command Line Interface

```

ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#tun
ciscoasa(config)#tunnel-group 210.210.2.2 ty
ciscoasa(config)#tunnel-group 210.210.2.2 type ip
ciscoasa(config)#tunnel-group 210.210.2.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#tun
ciscoasa(config)#tunnel-group 210.210.2.2 ip
ciscoasa(config)#tunnel-group 210.210.2.2 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#ike
ciscoasa(config-tunnel-ipsec)#ikev1 pre
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#

```

Copy Paste

Time: 27:25:42 Power Cycle Devices Fast Forward Time

Realtime

Connections

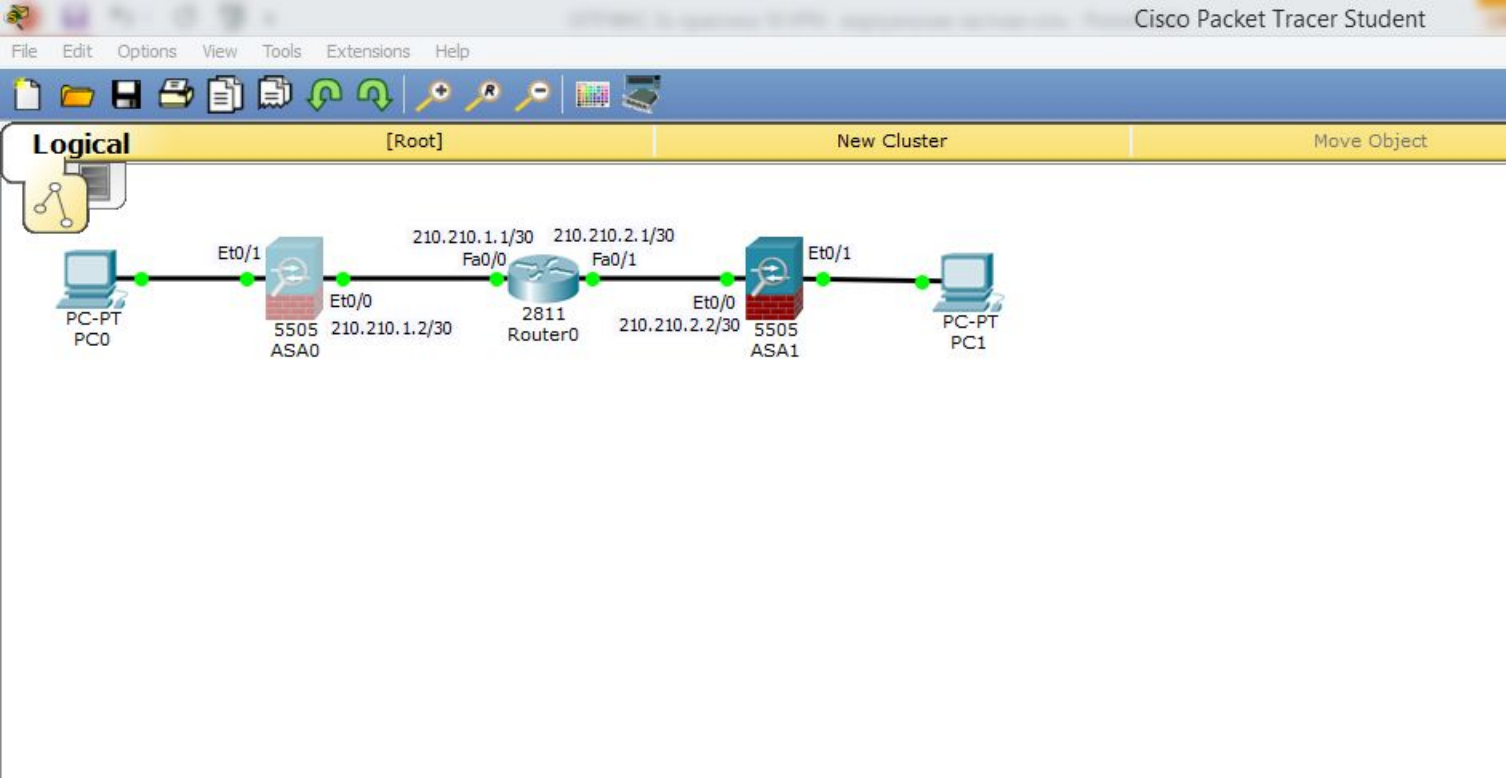
Copper Straight-Through

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete



```
ASA0
Physical Config CLI
ASA Command Line Interface
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ciscoasa(config)#
ciscoasa(config)#tun
ciscoasa(config)#tunnel-group 210.210.2.2 ip
ciscoasa(config)#tunnel-group 210.210.2.2 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#ike
ciscoasa(config-tunnel-ipsec)#ikev1 pre
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#cry
ciscoasa(config)#crypto ip
ciscoasa(config)#crypto ipsec ike
ciscoasa(config)#crypto ipsec ikev1 tr
ciscoasa(config)#crypto ipsec ikev1 transform-set ep-3
ciscoasa(config)#crypto ipsec ikev1 transform-set esp-3
ciscoasa(config)#crypto ipsec ikev1 transform-set TS esp-3des esp-m
ciscoasa(config)#crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac
ciscoasa(config)#
ciscoasa(config)#
```

Указываем параметры для построения ipsec-туннеля с именем TS, далее указываем алгоритм шифрования и хэширования: «crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac».

Time: 27:32:03 Power Cycle Devices Fast Forward Time Realtime

Connections

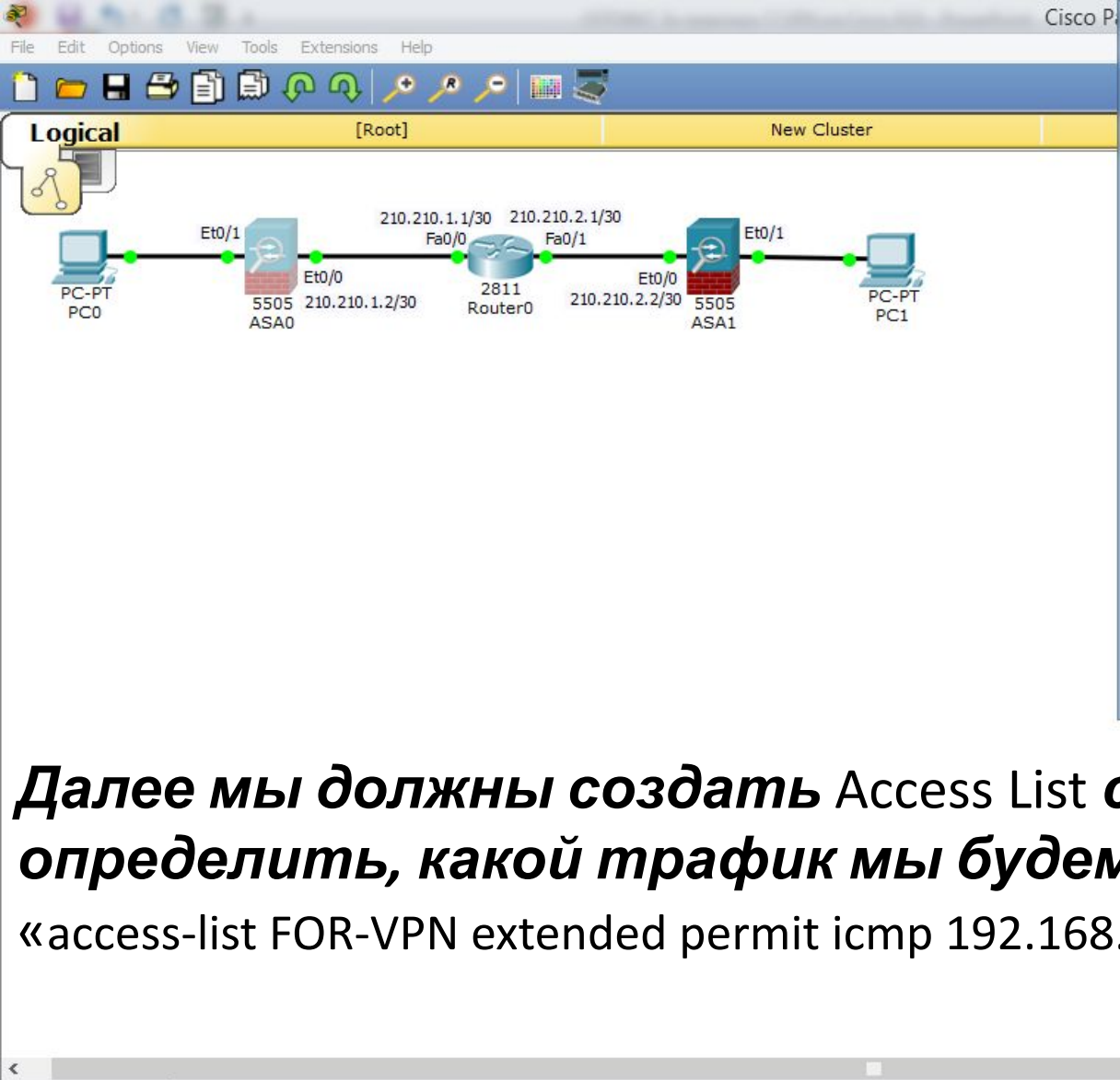
Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Toggle PDU List Window

Copper Straight-Through

Windows taskbar: 0:25 24.01.2020



```

ASA Command Line Interface
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#cry
ciscoasa(config)#crypto ip
ciscoasa(config)#crypto ipsec ike
ciscoasa(config)#crypto ipsec ikev1 tr
ciscoasa(config)#crypto ipsec ikev1 transform-set ep-3
ciscoasa(config)#crypto ipsec ikev1 transform-set esp-3
ciscoasa(config)#crypto ipsec ikev1 transform-set TS esp-3des esp-m
ciscoasa(config)#crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#acc
ciscoasa(config)#access-1
ciscoasa(config)#access-list FOR-VPN ext
ciscoasa(config)#access-list FOR-VPN extended her
ciscoasa(config)#access-list FOR-VPN extended per
ciscoasa(config)#access-list FOR-VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
ciscoasa(config)#
ciscoasa(config)#
  
```

Далее мы должны создать Access List с именем FOR-VPN, то есть определить, какой трафик мы будем направлять в VPN -туннель:
 «access-list FOR-VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0».

Time: 27:38:01 Power Cycle Devices Fast Forward Time Realtime

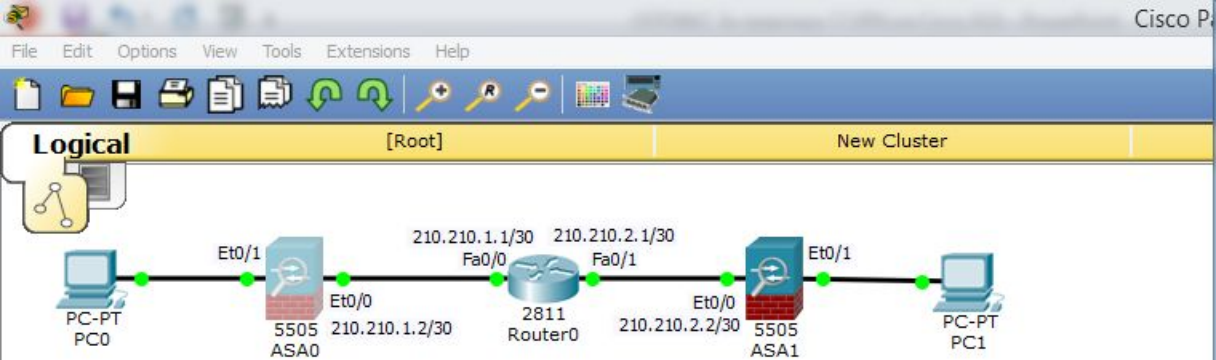
Connections

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
Toggle PDU List Window										

Copper Straight-Through

Windows taskbar: 0:31 24.01.2020



```
ASA Command Line Interface
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#acc
ciscoasa(config)#access-1
ciscoasa(config)#access-list FOR-VPN ext
ciscoasa(config)#access-list FOR-VPN extended her
ciscoasa(config)#access-list FOR-VPN extended per
ciscoasa(config)#access-list FOR-VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#cry
ciscoasa(config)#crypto map TO-SITE2 1 match address FOR-VPN
ciscoasa(config)#crypto map TO-SITE2 1 set peer 210.210.2.2
ciscoasa(config)#crypto map TO-SITE2 1 set secu
ciscoasa(config)#crypto map TO-SITE2 1 set security-association lif
ciscoasa(config)#crypto map TO-SITE2 1 set security-association lifetime seconds 86400
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE2 1 set ike
ciscoasa(config)#crypto map TO-SITE2 1 set ikev1 tr
ciscoasa(config)#crypto map TO-SITE2 1 set ikev1 transform-set TS
ciscoasa(config)#
ciscoasa(config)#
```

Создаём крипто-карту с именем TO-SITE2 под номером 1:

**«crypto map TO-SITE2 1 match address FOR-VPN»,
указываем пир, то есть внешний ip-адрес межсетевого экрана ASA1:
«crypto map TO-SITE2 1 set peer 210.210.2.2», и указываем lifetime туннеля в секундах:
«crypto map TO-SITE2 1 set security-association lifetime seconds 86400».
Привязываем transform-set TS: «crypto map TO-SITE2 1 set ikev1 transform-set TS».**

Time: 27:59:00 Power Cycle Devices Fast Forward Time Realtime

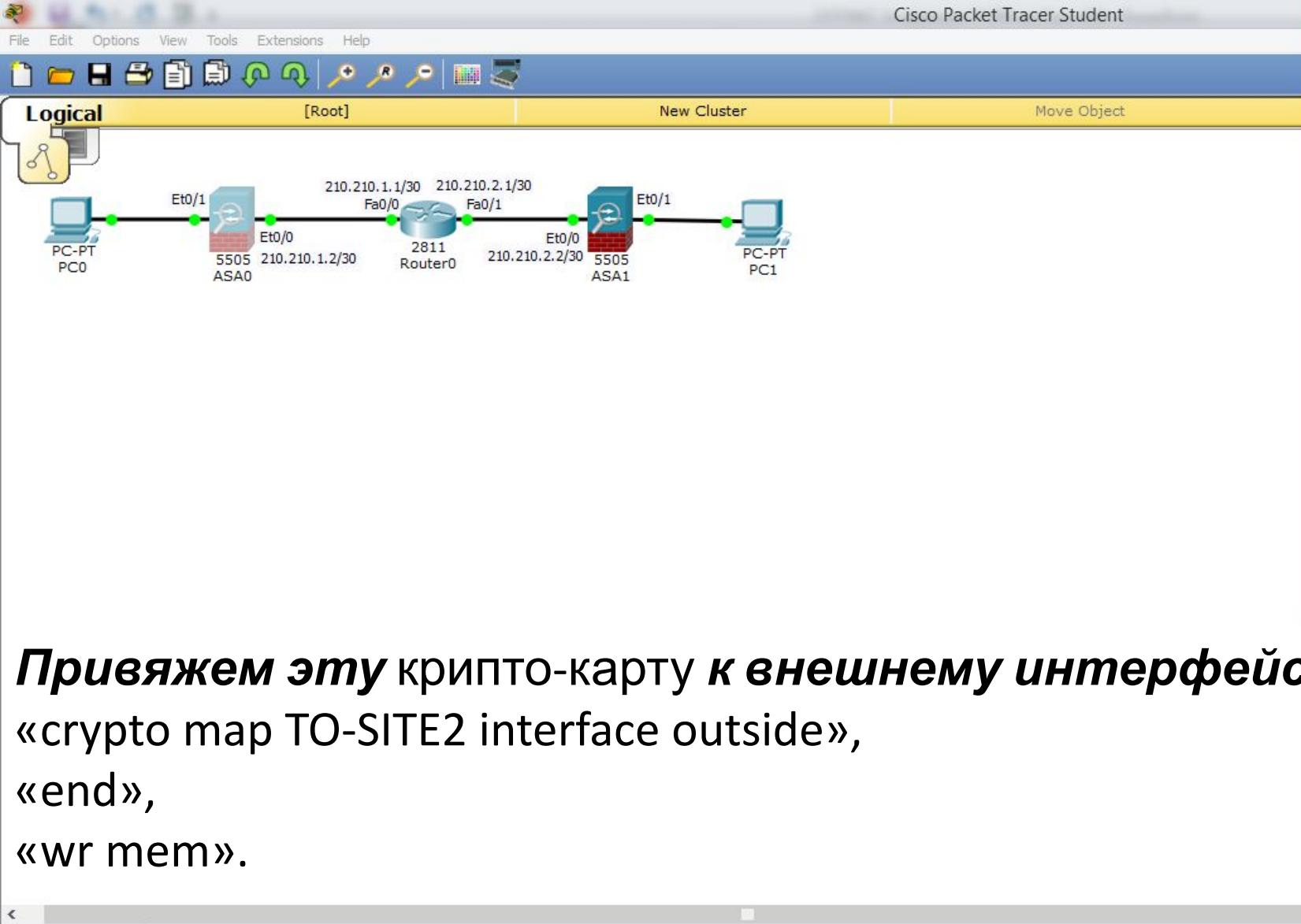
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete

Scenario 0 New Delete Toggle PDU List Window

Copper Straight-Through

Windows taskbar: Internet Explorer, File Explorer, Microsoft Word, Firefox, Microsoft Excel, Google Chrome, Microsoft PowerPoint, VLC media player.

System tray: ENG, 0:52, 24.01.2020



```
ASA0
Physical Config CLI
ASA Command Line Interface
ciscoasa(config)#crypto map TO-SITE2 1 set security-association lif
ciscoasa(config)#crypto map TO-SITE2 1 set security-association
lifetime seconds 86400
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE2 1 set ike
ciscoasa(config)#crypto map TO-SITE2 1 set ikev1 tr
ciscoasa(config)#crypto map TO-SITE2 1 set ikev1 transform-set TS
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE2 in
ciscoasa(config)#crypto map TO-SITE2 interface out
ciscoasa(config)#crypto map TO-SITE2 interface outside
WARNING: crypto map has incomplete entries
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 3c8246d4 3f837647 3f331ad0 1dc13e50

1536 bytes copied in 1.154 secs (1331 bytes/sec)
[OK]
ciscoasa#
ciscoasa#
```

Привяжем эту крипто-карту **к внешнему интерфейсу:**
«crypto map TO-SITE2 interface outside»,
«end»,
«wr mem».

Time: 28:02:57 Power Cycle Devices Fast Forward Time **Realtime**

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Connections

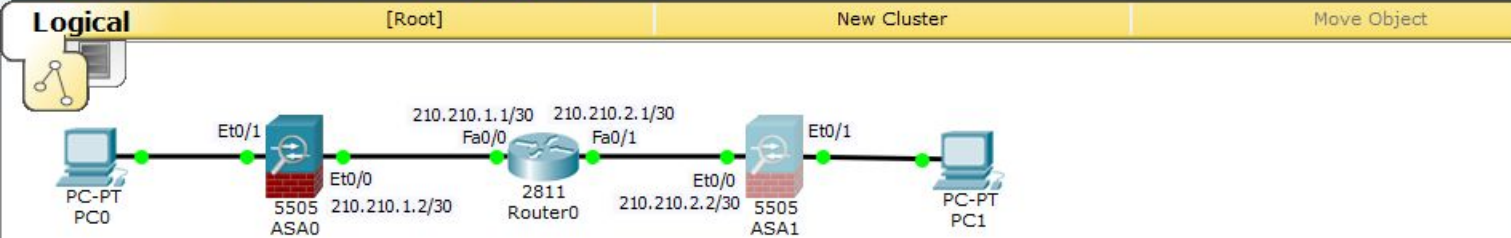
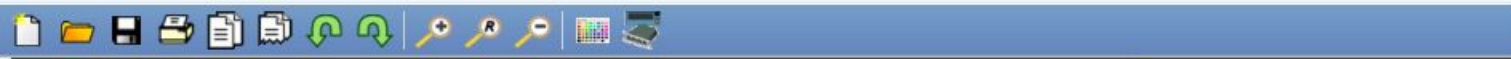
Copper Straight-Through

New Delete

Toggle PDU List Window

Windows taskbar: Internet Explorer, File Explorer, Microsoft Word, Firefox, Microsoft Excel, PowerPoint, VLC media player

System tray: ENG, 0:56, 24.01.2020



Начнём с маршрутизатора центрального офиса Router0. Для начала нам необходимо настроить первую фазу. На внешнем интерфейсе включим протокол ike: «crypto ikev1 enable outside»

Далее создаётся политика: «crypto ikev1 policy 1» где мы указываем алгоритм шифрования 3des (это параметры для построения мини туннеля ISAKMP-туннеля, через который будут передаваться параметры основного Ipsec-туннеля): «encryption 3des», алгоритм хеширования md5: «hash md5», тип аутентификации Pre-Shared Key: «authentication pre-share» и алгоритм Диффи – Хеллмана: «group 2», «exit»

```
ASA1
Physical Config CLI
ASA Command Line Interface
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 26000853 07a73a53 6ee76e33 1b801986

938 bytes copied in 1.45 secs (646 bytes/sec)
[OK]
ciscoasa#
ciscoasa#
ciscoasa#conf t
ciscoasa(config)#crypto ikev1 enable outside
ciscoasa(config)#
ciscoasa(config)#crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)#
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#
ciscoasa(config-ikev1-policy)#hash md5
ciscoasa(config-ikev1-policy)#
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#
ciscoasa(config-ikev1-policy)#exit
ciscoasa(config)#
```

Copy Paste

Power Cycle Devices Fast Forward Time Realtime

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

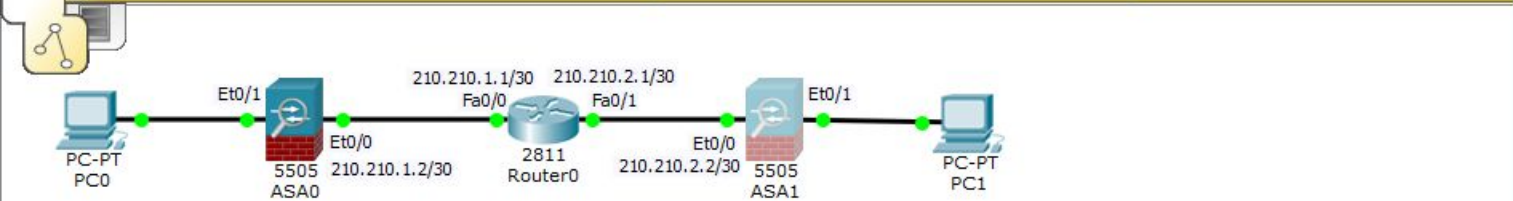
New Delete Toggle PDU List Window

Copper Straight-Through

Windows taskbar with icons for Internet Explorer, File Explorer, Word, Firefox, Excel, PowerPoint, and other applications. System tray shows date and time: 1:06 24.01.2020.



Logical [Root] New Cluster Move Object



ASA1

Physical Config CLI

ASA Command Line Interface

```
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#tunnel-group 210.210.1.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ciscoasa(config)#tunnel-group 210.210.1.2 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac
ciscoasa(config)#
```

Copy Paste

Указываем параметры для построения ipsec-туннеля с именем TS, далее указываем алгоритм шифрования и хэширования: «crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac».

Time: 28:21:13 Power Cycle Devices Fast Forward Time

Connections

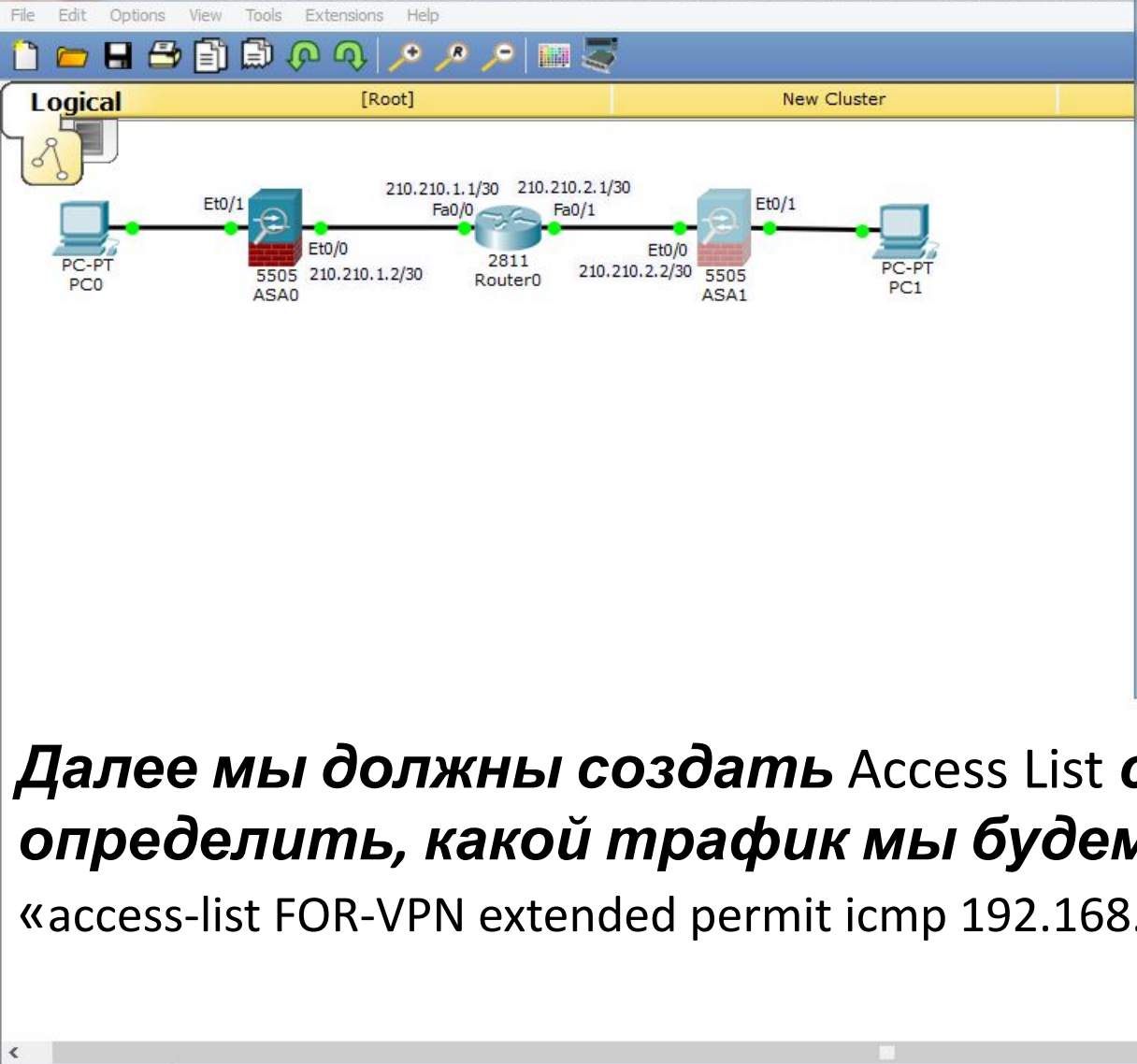
Copper Straight-Through

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete



```
Physical Config CLI
ASA Command Line Interface
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#tunnel-group 210.210.1.2 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ciscoasa(config)#tunnel-group 210.210.1.2 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#access-list FOR-VPN extended permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
ciscoasa(config)#
ciscoasa(config)#
```

Copy Paste

Далее мы должны создать Access List с именем FOR-VPN, то есть определить, какой трафик мы будем направлять в VPN -туннель:
«access-list FOR-VPN extended permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0».

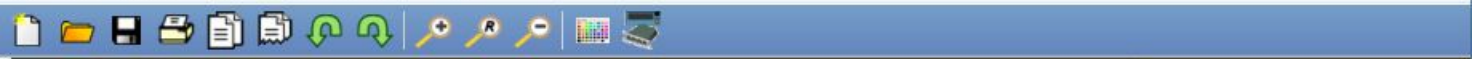
Time: 28:23:25 Power Cycle Devices Fast Forward Time Realtime

Scenario 0

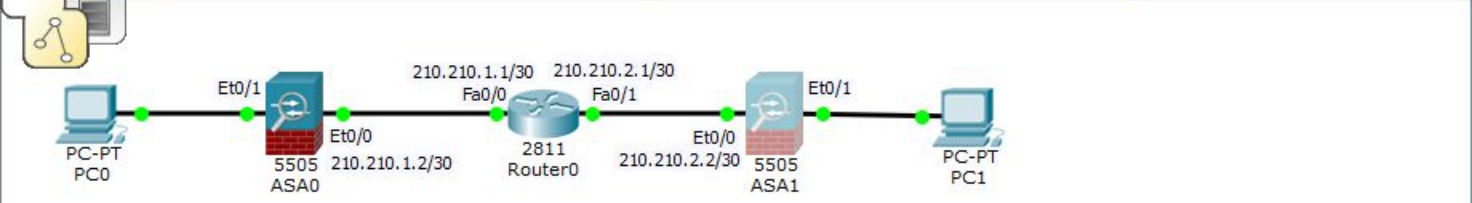
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
Toggle PDU List Window										

Connections: Copper Straight-Through

Windows taskbar: ENG 1:17 24.01.2020



Logical [Root] New Cluster Move Object



ASA1

Physical Config CLI

ASA Command Line Interface

```

ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
ciscoasa(config-tunnel-ipsec)#
ciscoasa(config-tunnel-ipsec)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#crypto ipsec ikev1 transform-set TS esp-3des esp-md5-hmac
ciscoasa(config)#
ciscoasa(config)#access-list FOR-VPN extended permit icmp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 match address FOR-VPN
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 set peer 210.210.1.2
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 set security-association lifetime seconds 86400
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 set ikev1 transform-set TS
ciscoasa(config)#
ciscoasa(config)#
  
```

Copy Paste

Создаём крипто-карту **с именем TO-SITE2** **под номером 1:**

«crypto map TO-SITE1 1 match address FOR-VPN»,

указываем пир, то есть внешний ip-адрес межсетевого экрана ASA1:

«crypto map TO-SITE1 1 set peer 210.210.1.2», **и указываем lifetime туннеля в секундах:** «crypto map TO-SITE1 1 set security-association lifetime seconds 86400».

Привязываем transform-set TS: «crypto map TO-SITE1 1 set ikev1 transform-set TS».

Time: 28:28:44 Power Cycle Devices Fast Forward Time Realtime

Connections

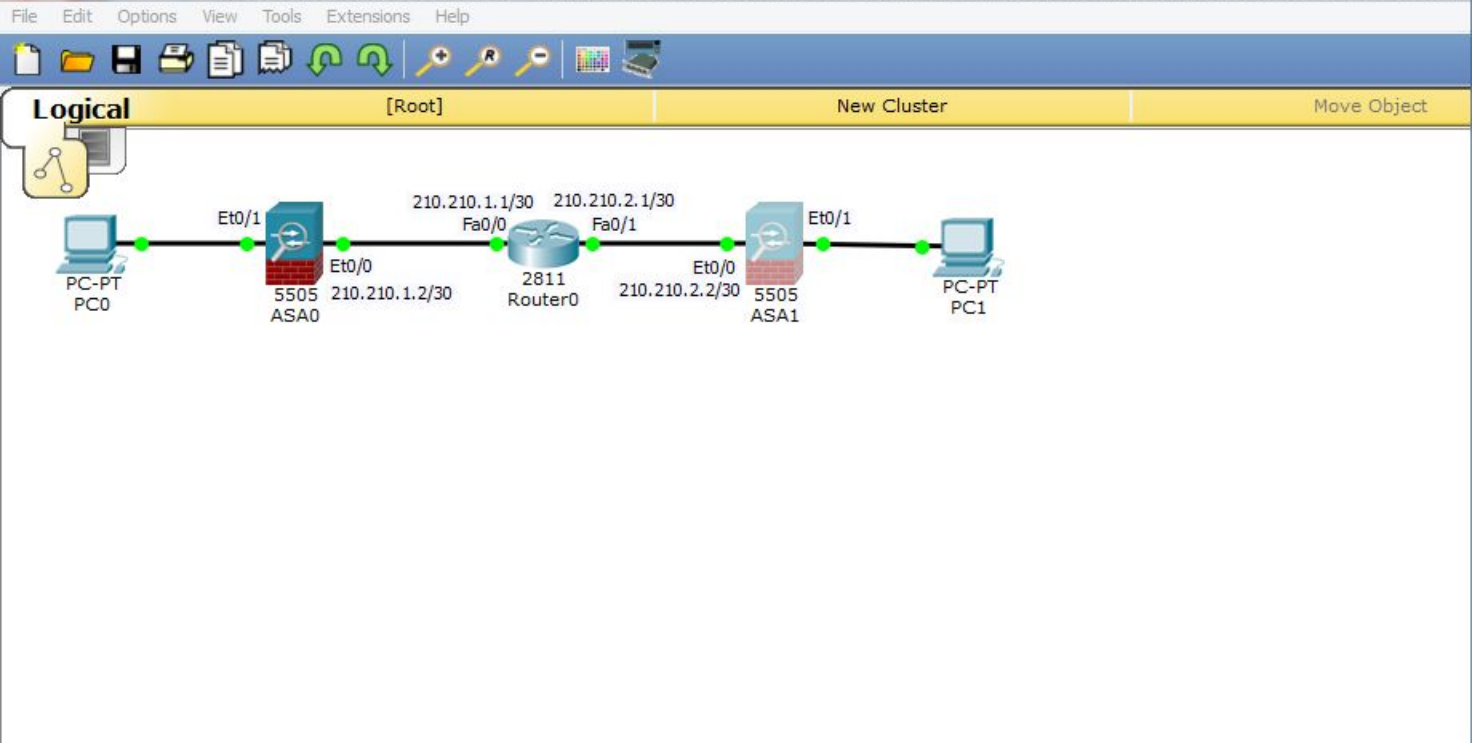
Copper Straight-Through

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete



```
ASA1
Physical Config CLI
ASA Command Line Interface
ciscoasa(config)#crypto map TO-SITE1 1 set peer 210.210.1.2
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 set security-association lifetime seconds 86400
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 1 set ikev1 transform-set TS
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#crypto map TO-SITE1 interface outside
WARNING: crypto map has incomplete entries
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 26000853 07a73a53 6ee76e33 1b801986

1575 bytes copied in 1.866 secs (844 bytes/sec)
[OK]
ciscoasa#
ciscoasa#
```

Привяжем эту крипто-карту **к внешнему интерфейсу:**

«crypto map TO-SITE1 interface outside»,

«end»,

«wr mem».

Time: 28:31:19 Power Cycle Devices Fast Forward Time

Realtime

Connections

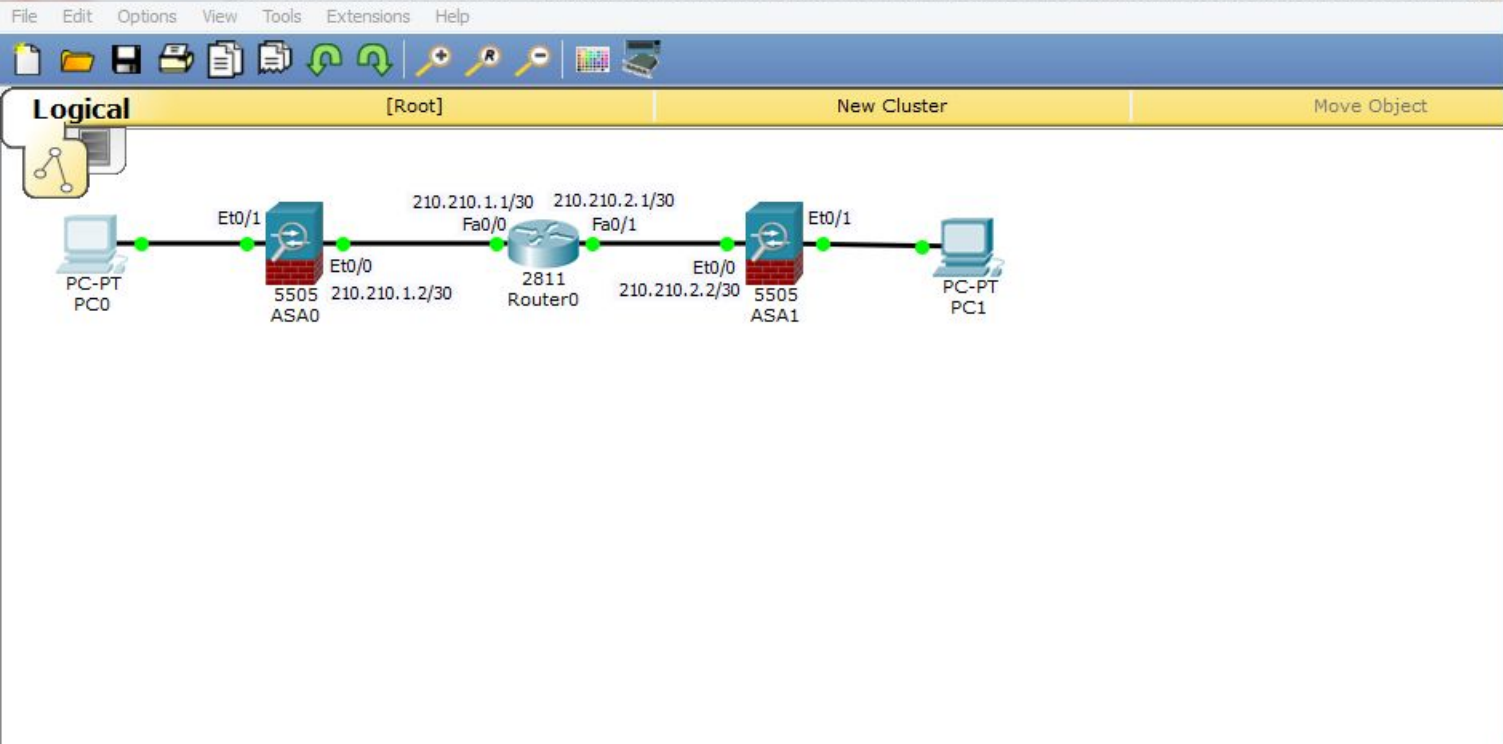
Copper Straight-Through

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Проверим связь между компьютерами из центрального офиса и филиала:

«ping 192.168.2.5».

Связи нет 😞

Time: 48:59:04 Power Cycle Devices Fast Forward Time

Realtime

Connections

Copper Straight-Through

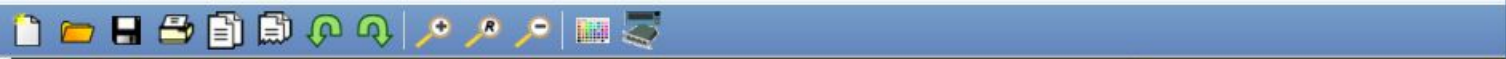
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete

Scenario 0

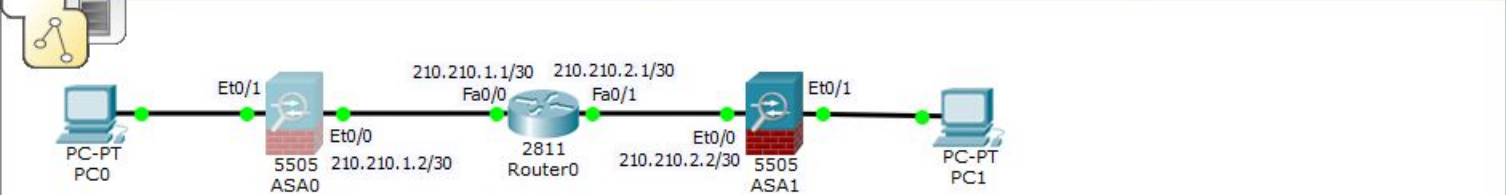
New Delete

Toggle PDU List Window

Windows taskbar with icons for Internet Explorer, File Explorer, Microsoft Store, Windows Defender, Word, Firefox, Excel, Chrome, PowerPoint, and a folder icon.



Logical [Root] New Cluster Move Object



ASA0

Physical Config CLI

ASA Command Line Interface

```
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 3c8246d4 3f837647 3f331ad0 1dc13e50

1536 bytes copied in 1.154 secs (1331 bytes/sec)
[OK]
ciscoasa#
ciscoasa#show cry
ciscoasa#show crypto isa
ciscoasa#show crypto isakmp sa

IKEv1 SAs:
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1
1 IKE Peer: 210.210.2.2
  Type    : L2L           Role    : Initiator
  Rekey   : no          State   : MM NO STATE

There are no IKEv2 SAs
ciscoasa#
```

Copy Paste

Зайдём на ASA0. Посмотрим, строится ли туннель:

«show crypto isakmp sa».

Видим, что технологический туннель построен.

Time: 49:04:17 Power Cycle Devices Fast Forward Time

Realtime

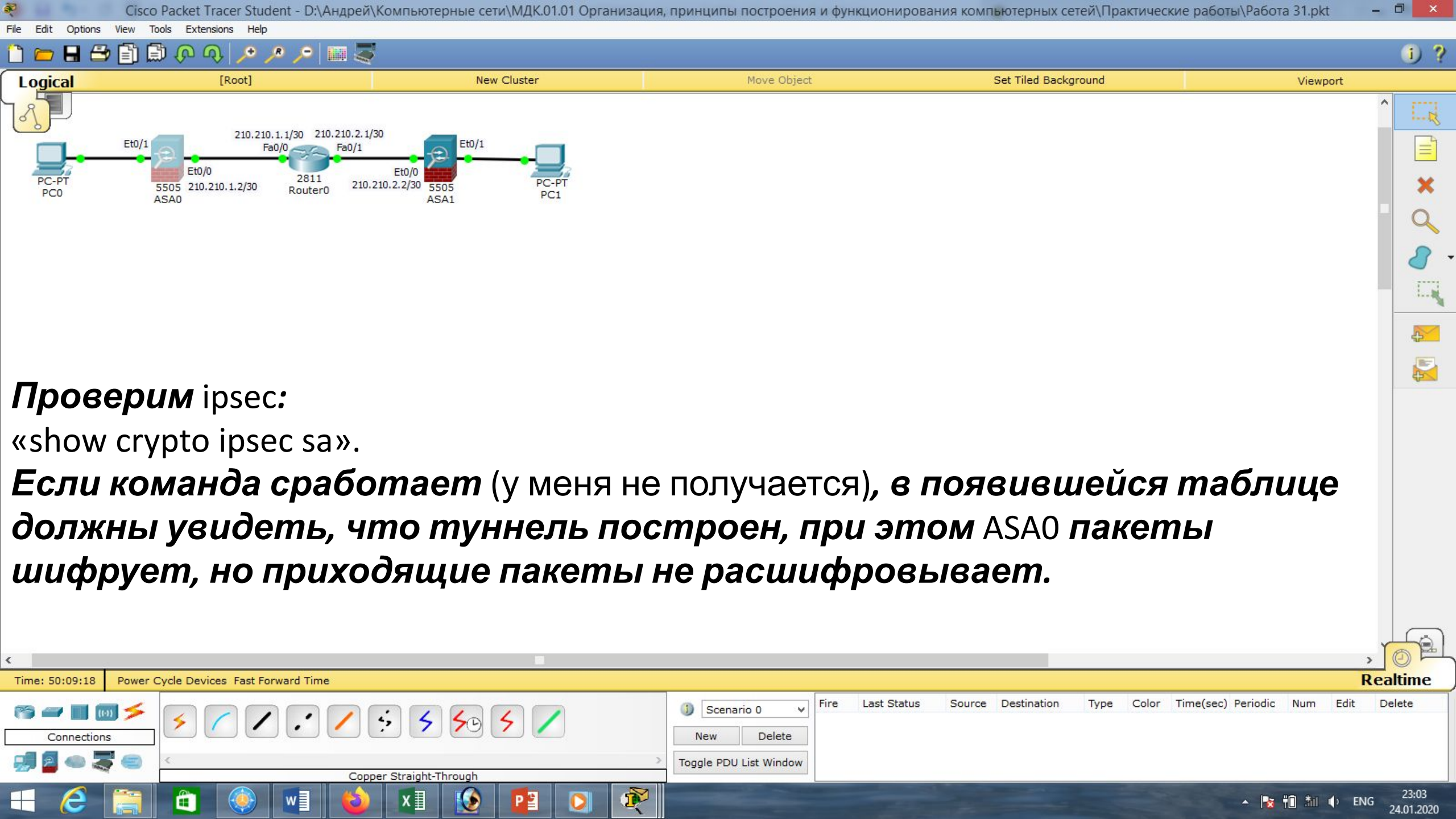
Connections

Scenario 0

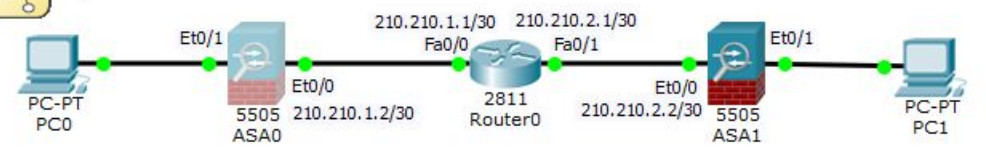
New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------



Logical [Root] New Cluster Move Object Set Tiled Background Viewport



Проверим ipsec:

«show crypto ipsec sa».

Если команда сработает (у меня не получается), в появившейся таблице должны увидеть, что туннель построен, при этом ASA0 пакеты шифрует, но входящие пакеты не расшифровывает.

Time: 50:09:18 Power Cycle Devices Fast Forward Time

Realtime

Connections

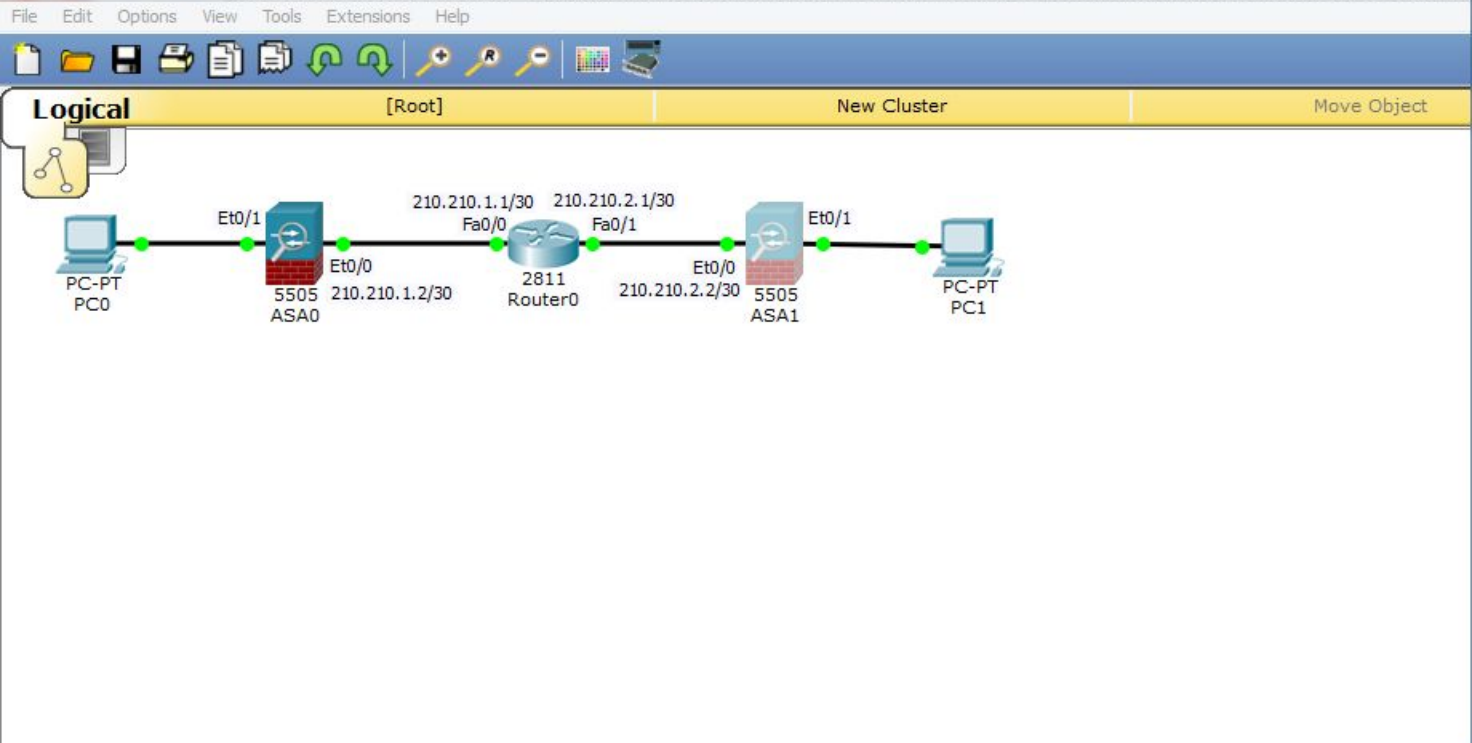
Copper Straight-Through

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete



```
ASA1
Physical Config CLI
ASA Command Line Interface
ciscoasa#show ip
ciscoasa#show ip cry
ciscoasa#show ip cryp
ciscoasa#show cryp
ciscoasa#show crypto ip
ciscoasa#show crypto ipsec sa

There are no ipsec sas
ciscoasa#show crypto isakmp sa

IKEv1 SAs:
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1
1 IKE Peer: 210.210.1.2
  Type : L2L           Role : responder
  Rekey : no           State : QM_IDLE

There are no IKEv2 SAs
ciscoasa#
ciscoasa#
ciscoasa#
```

Зайдём на ASA1. Посмотрим, строится ли туннель:

«show crypto isakmp sa».

Видим, что технологический туннель построен.

Time: 49:24:06 Power Cycle Devices Fast Forward Time

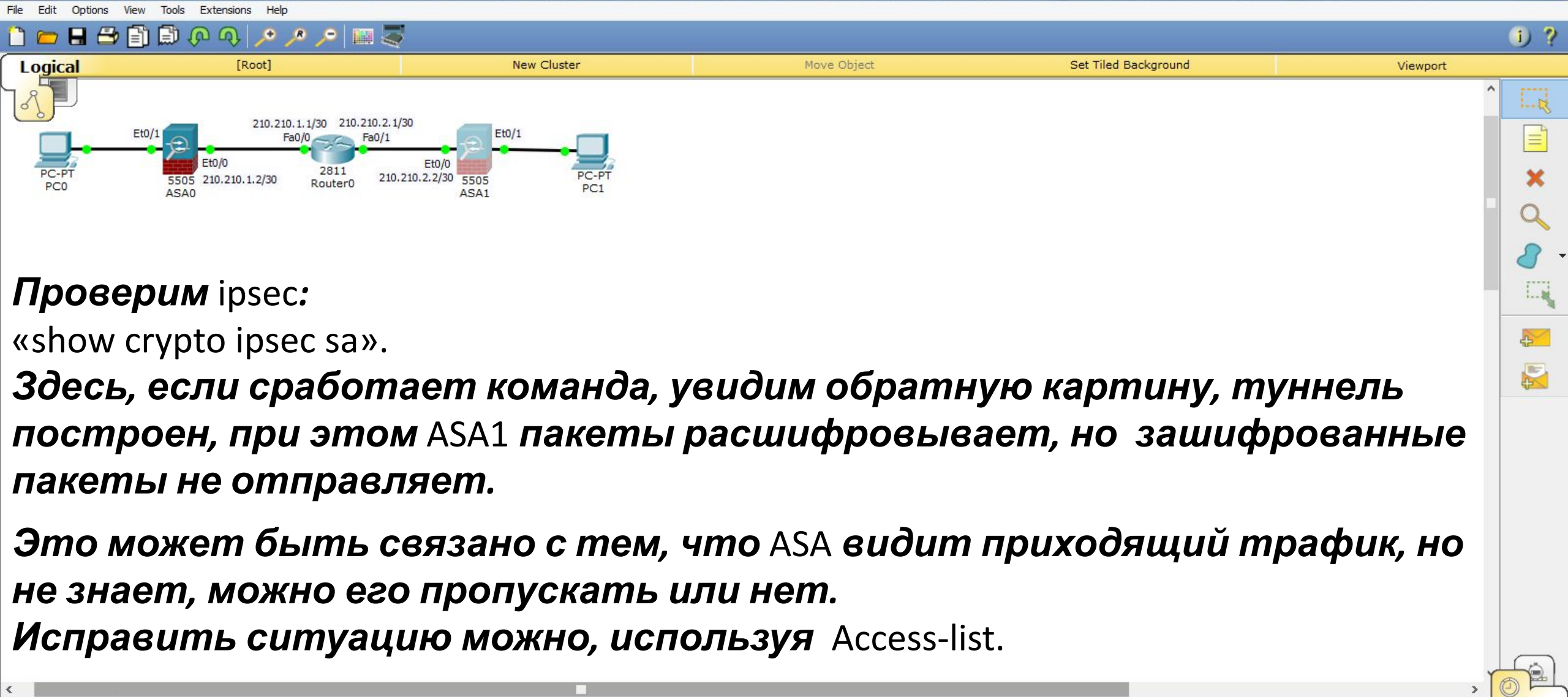
Realtime

Connections

Copper Straight-Through

Scenario 0	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
New	Delete									
Toggle PDU List Window										

Windows taskbar with icons for Internet Explorer, File Explorer, Microsoft Word, Firefox, Microsoft Excel, and other applications.



Проверим ipsec:

«show crypto ipsec sa».

Здесь, если сработает команда, увидим обратную картину, туннель построен, при этом ASA1 пакеты расшифровывает, но зашифрованные пакеты не отправляет.

Это может быть связано с тем, что ASA видит входящий трафик, но не знает, можно его пропускать или нет.

Исправить ситуацию можно, используя Access-list.

Time: 50:12:48 Power Cycle Devices Fast Forward Time **Realtime**

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

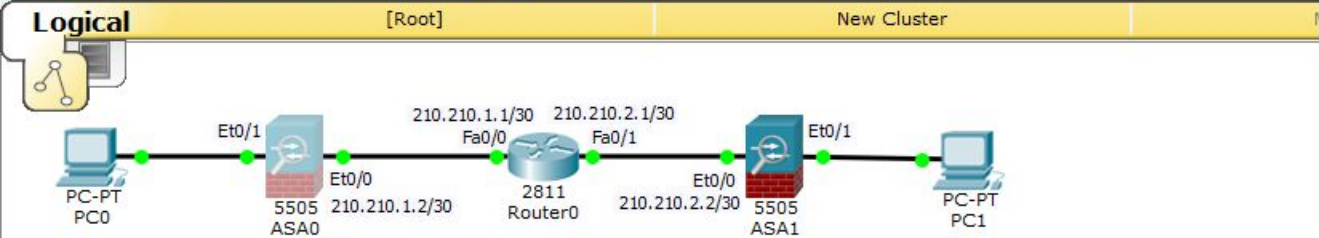
Connections

Copper Straight-Through

New Delete

Toggle PDU List Window

Windows taskbar: 23:07 24.01.2020



Создадим такой Access-list на ASA0 с именем FROM-VPN и разрешим трафик из сети 192.168.2.0, получателем будет сеть 192.168.1.0 :

«access-list FROM-VPN permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0».

Привяжем это Access-list на исходящий интерфейс ASA0. Для трафика из сети 192.168.2.0 входящим в ASA0 будет интерфейс Et0/0, а исходящим – Et0/1 (то есть, к компьютерам) :

«access-group FROM-VPN out interface inside», «end», «wr mem».

ASA0

Physical Config CLI

ASA Command Line Interface

```

#####
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/14 ms

ciscoasa(config)#acc
ciscoasa(config)#access
ciscoasa(config)#access-li
ciscoasa(config)#access-list FROM-VPN per
ciscoasa(config)#access-list FROM-VPN permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
ciscoasa(config)#
ciscoasa(config)#access-g
ciscoasa(config)#access-group FROM-VPN out in
ciscoasa(config)#access-group FROM-VPN out interface in
ciscoasa(config)#access-group FROM-VPN out interface inside
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 3c8246d4 3f837647 3f331ad0 1dc13e50

1671 bytes copied in 1.18 secs (1416 bytes/sec)
[OK]
ciscoasa#
  
```

Copy Paste

Time: 50:39:55 Power Cycle Devices Fast Forward Time

Realtime

Connections

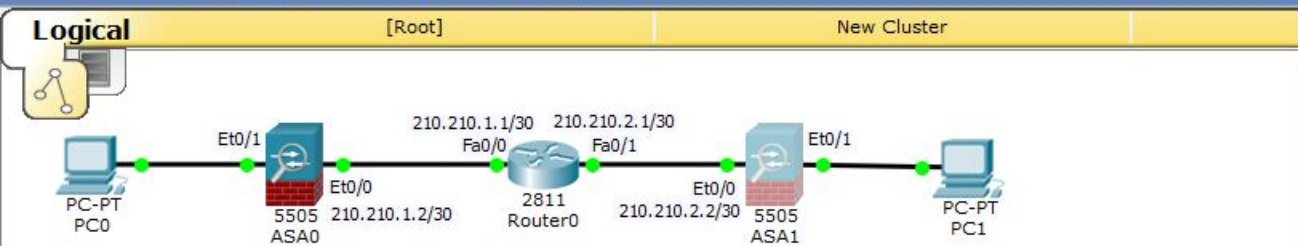
Copper Straight-Through

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete



Аналогичные действия проведём на ASA1.

Создадим Access-list с именем FROM-VPN и разрешим трафик из сети

192.168.1.0, получателем будет сеть

192.168.2.0:

«access-list FROM-VPN permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0».

Привяжем это Access-list на исходящий интерфейс ASA1. Для трафика из сети 192.168.1.0 входящим в ASA0 будет интерфейс Et0/0, а исходящим – Et0/1 (то есть, к компьютерам):

«access-group FROM-VPN out interface inside», «end», «wr mem».

ASA1

Physical Config CLI

ASA Command Line Interface

```

ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#access-list FROM-VPN permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
ciscoasa(config)#
ciscoasa(config)#access-group FROM-VPN out interface inside
ciscoasa(config)#
ciscoasa(config)#end
ciscoasa#
ciscoasa#wr mem
Building configuration...
Cryptochecksum: 26000853 07a73a53 6ee76e33 1b801986

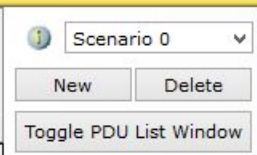
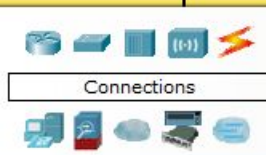
1710 bytes copied in 2.145 secs (797 bytes/sec)
[OK]
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#

```

Copy Paste

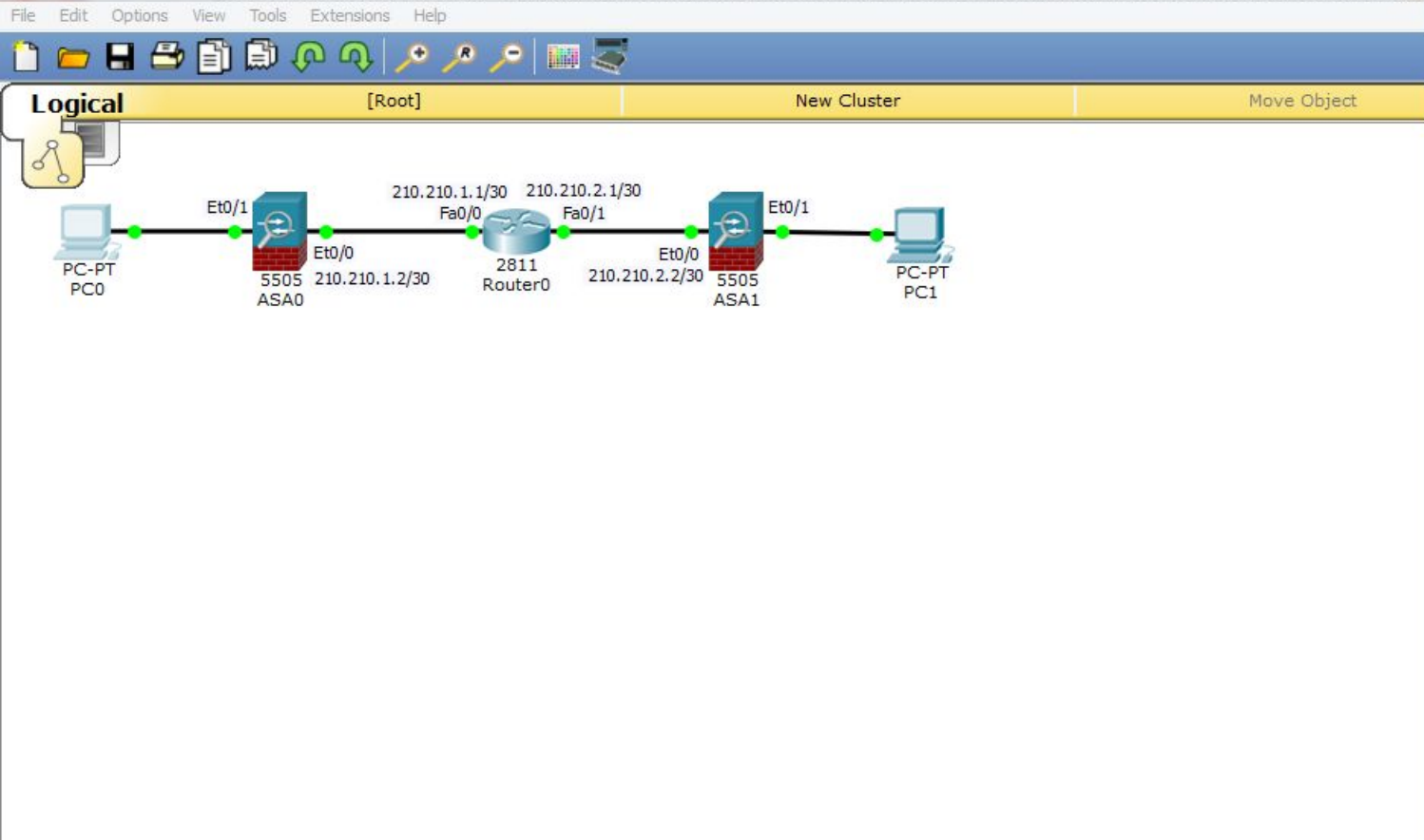
Time: 50:49:22 Power Cycle Devices Fast Forward Time

Realtime



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete





```
PC>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:

Reply from 192.168.2.5: bytes=32 time=11ms TTL=126
Reply from 192.168.2.5: bytes=32 time=14ms TTL=126
Reply from 192.168.2.5: bytes=32 time=11ms TTL=126
Reply from 192.168.2.5: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 14ms, Average = 12ms

PC>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:

Reply from 192.168.2.5: bytes=32 time=15ms TTL=126
Reply from 192.168.2.5: bytes=32 time=10ms TTL=126
Reply from 192.168.2.5: bytes=32 time=11ms TTL=126
Reply from 192.168.2.5: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 15ms, Average = 11ms

PC>
```

**Проверим связь между компьютерами из Центрального офиса и филиала:
«ping 192.168.2.5».
Связь есть!!!**

Time: 50:55:12 Power Cycle Devices Fast Forward Time **Realtime**

Connections

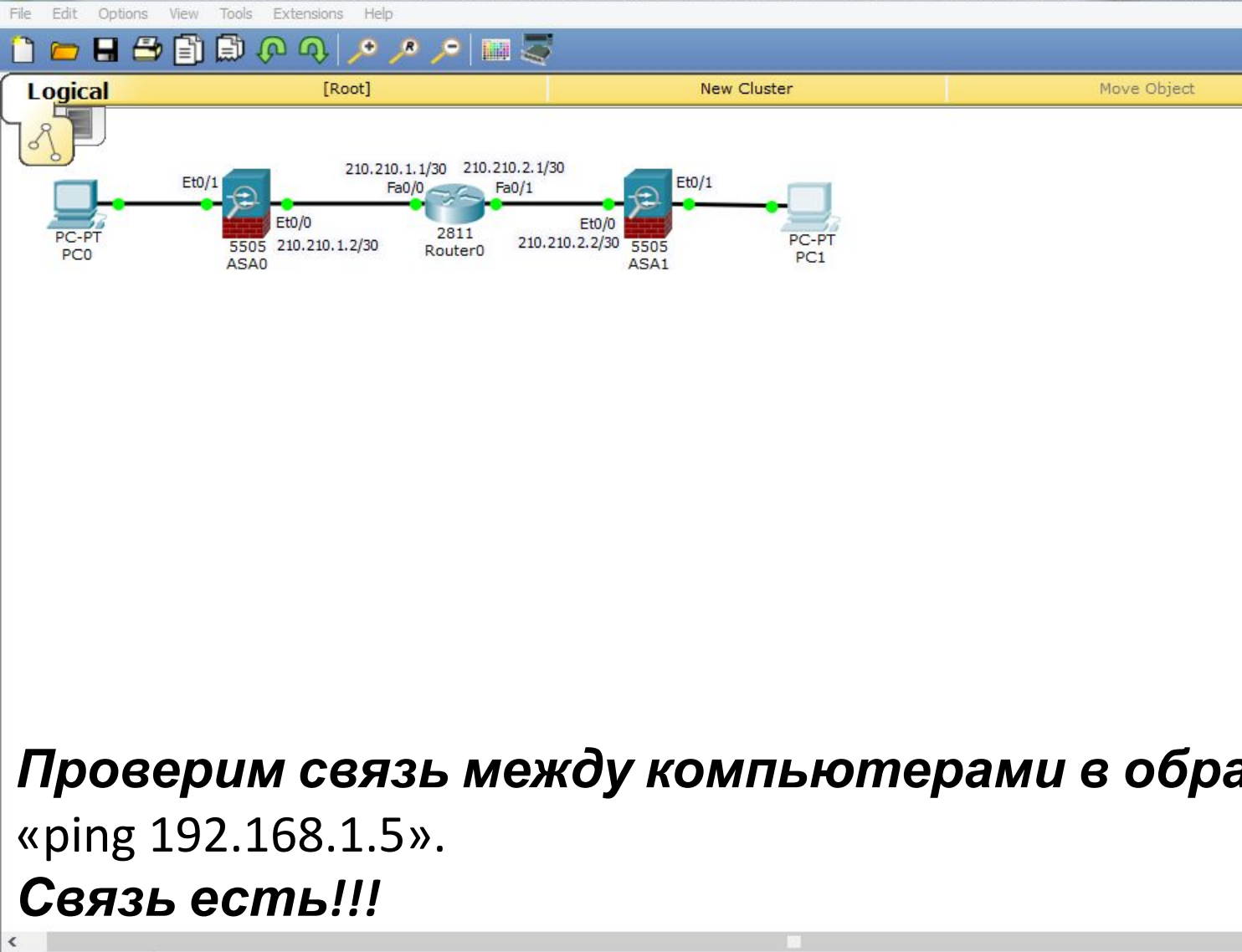
Copper Straight-Through

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

New Delete Toggle PDU List Window

Windows taskbar: 23:50 24.01.2020



PC1

Physical Config Desktop Custom Interface

Command Prompt

```
PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=11ms TTL=126
Reply from 192.168.1.5: bytes=32 time=10ms TTL=126
Reply from 192.168.1.5: bytes=32 time=12ms TTL=126
Reply from 192.168.1.5: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 13ms, Average = 11ms

PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=10ms TTL=126
Reply from 192.168.1.5: bytes=32 time=11ms TTL=126
Reply from 192.168.1.5: bytes=32 time=11ms TTL=126
Reply from 192.168.1.5: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 12ms, Average = 11ms

PC>
```

Проверим связь между компьютерами в обратном направлении:
«ping 192.168.1.5».
Связь есть!!!

Time: 50:57:05 Power Cycle Devices Fast Forward Time

Connections

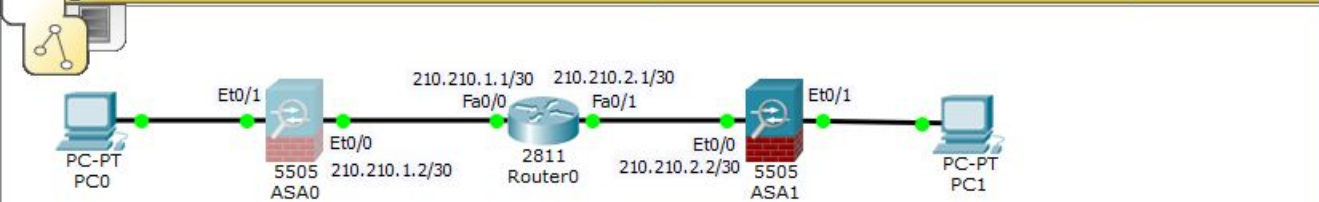
Copper Straight-Through

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Realtime

Windows taskbar: 23:51 24.01.2020



Зайдём на ASA0.

Ещё раз проверим ipsec:

«show crypto ipsec sa».

Туннель построен, при этом видим количество зашифрованных и расшифрованных пакетов.

ASA0

Physical Config CLI

ASA Command Line Interface

```

1671 bytes copied in 1.18 secs (1416 bytes/sec)
[OK]
ciscoasa#
ciscoasa#show crypto ipsec sa

interface: outside
  Crypto map tag: TO-SITE2, seq num: 1, local addr 210.210.1.2

  permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
  local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/1/0)
  remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/1/0)
  current_peer 210.210.2.2
  #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
  #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors 1, #recv errors 0

  local crypto endpt.: 210.210.1.2/0, remote crypto endpt.:210.210.2.2/0
  path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
  current outbound spi: 0x07AB0437(128648247)
  current inbound spi: 0x416A3D15(128648247)

inbound esp sas:

ciscoasa#
ciscoasa#
  
```

Copy Paste

Connections

Copper Straight-Through

Scenario 0

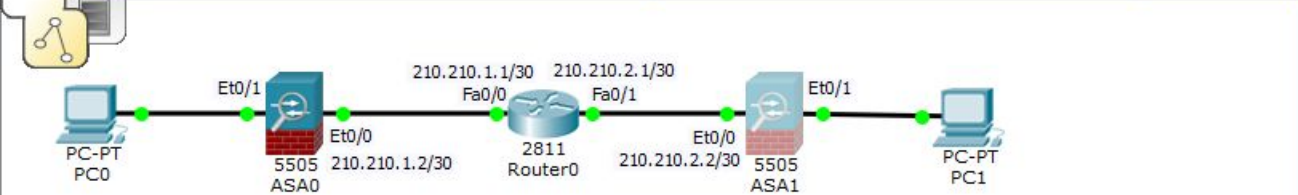
New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete



Logical [Root] New Cluster



Physical Config CLI

ASA Command Line Interface

```
ciscoasa#
ciscoasa#show crypto ipsec sa

interface: outside
  Crypto map tag: TO-SITE1, seq num: 1, local addr 210.210.2.2

  permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
  local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/1/0)
  remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/1/0)
  current peer 210.210.1.2
  #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 0
  #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 210.210.2.2/0, remote crypto endpt.:210.210.1.2/0
  path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500
  current outbound spi: 0x416A3D15(1097481493)
  current inbound spi: 0x07AB0437(1097481493)
```

Copy Paste

Зайдём на ASA1.

Тоже проверим ipsec:

«show crypto ipsec sa».

Туннель построен, тоже видим количество зашифрованных и расшифрованных пакетов.

Time: 51:04:24 Power Cycle Devices Fast Forward Time

Realtime

Connections

Copper Straight-Through

Scenario 0

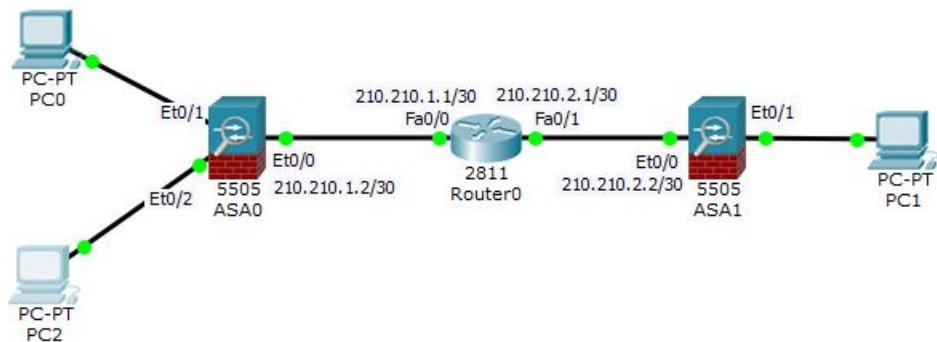
New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------



Logical [Root] New Cluster Move Object



PC2

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

DHCP Static DHCP request successful.

IP Address 192.168.1.6

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server

IPv6 Configuration

DHCP Auto Config Static

IPv6 Address

Link Local Address FE80::203:E4FF:FE82:8E24

IPv6 Gateway

IPv6 DNS Server

**Добавим компьютер в Центральный офис,
включим DHCP, получим ip-адрес.**

Time: 85:18:45 Power Cycle Devices Fast Forward Time

Realtime

Connections

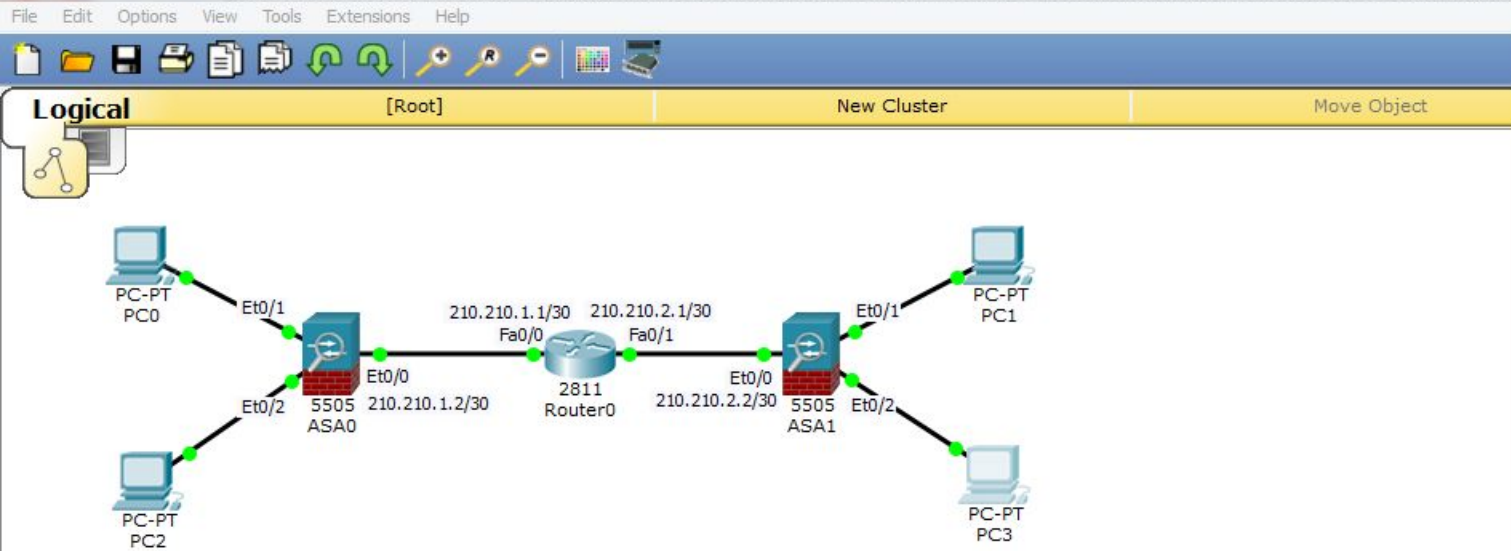
Copper Straight-Through

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------



Добавим компьютер в филиал, включим DHCP, получим ip-адрес.

PC3

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

DHCP Static DHCP request successful.

IP Address 192.168.2.6

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server

IPv6 Configuration

DHCP Auto Config Static

IPv6 Address

Link Local Address FE80::2D0:BCFF:FE31:257E

IPv6 Gateway

IPv6 DNS Server

Time: 85:25:39 Power Cycle Devices Fast Forward Time

Realtime

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Scenario 0

New Delete

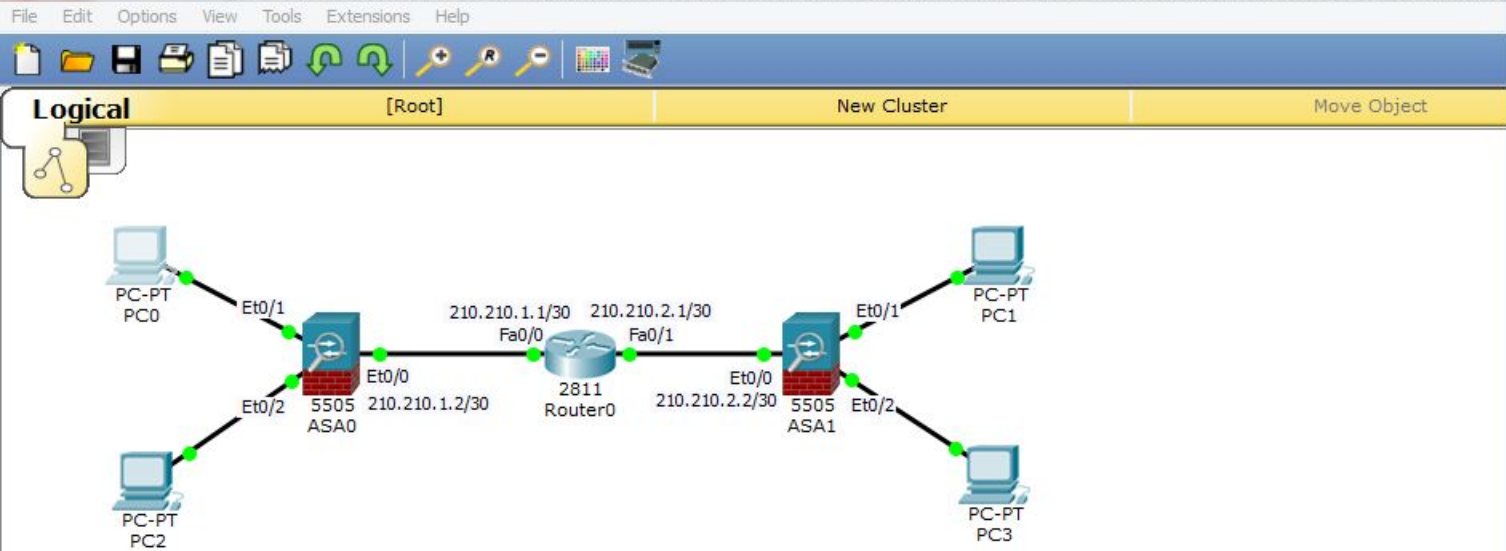
Toggle PDU List Window

WAN Emulation

Generic Generic DSL Modem Cable Modem

Copper Straight-Through

Windows Taskbar: Internet Explorer, File Explorer, Mail, Calendar, Word, Firefox, Excel, PowerPoint, Media Center, Network, Volume, CPU, Memory, Network, System Tray, 10:20 25.01.2020



```
PC0
```

Physical Config Desktop Custom Interface

Command Prompt

```
PC>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:

Reply from 192.168.2.5: bytes=32 time=15ms TTL=126
Reply from 192.168.2.5: bytes=32 time=10ms TTL=126
Reply from 192.168.2.5: bytes=32 time=11ms TTL=126
Reply from 192.168.2.5: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 15ms, Average = 11ms

PC>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.2.5: bytes=32 time=11ms TTL=126
Reply from 192.168.2.5: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 11ms, Average = 11ms

PC>ping 192.168.2.5
```

Ещё раз проверим связь между компьютерами из Центрального офиса и филиала:
«ping 192.168.2.5».

Связь не сразу, но появляется.

Realtime

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------

Scenario 0

New Delete

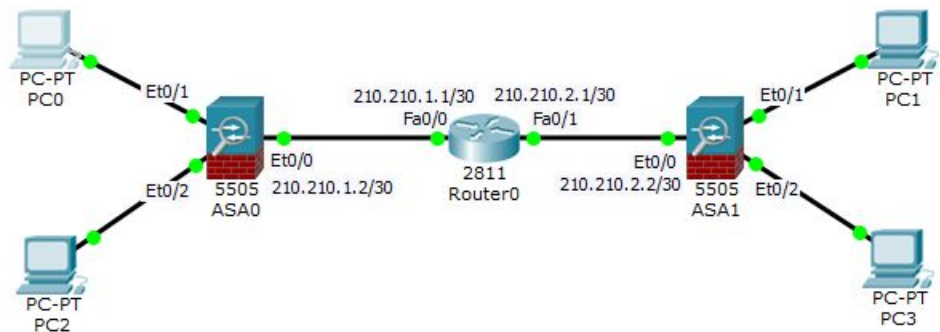
Toggle PDU List Window

WAN Emulation

Generic Generic DSL Modem Cable Modem

Copper Straight-Through

10:25 25.01.2020



PC0

Physical Config Desktop Custom Interface

Command Prompt

```
PC>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=10ms TTL=126
Reply from 192.168.2.6: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 14ms, Average = 11ms

PC>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=12ms TTL=126
Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=24ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 24ms, Average = 14ms

PC>
```

Проверим связь между компьютером из Центрального офиса и добавленным компьютером филиала: «ping 192.168.2.6».
Связь есть!!!

Time: 85:33:10 Power Cycle Devices Fast Forward Time

Realtime

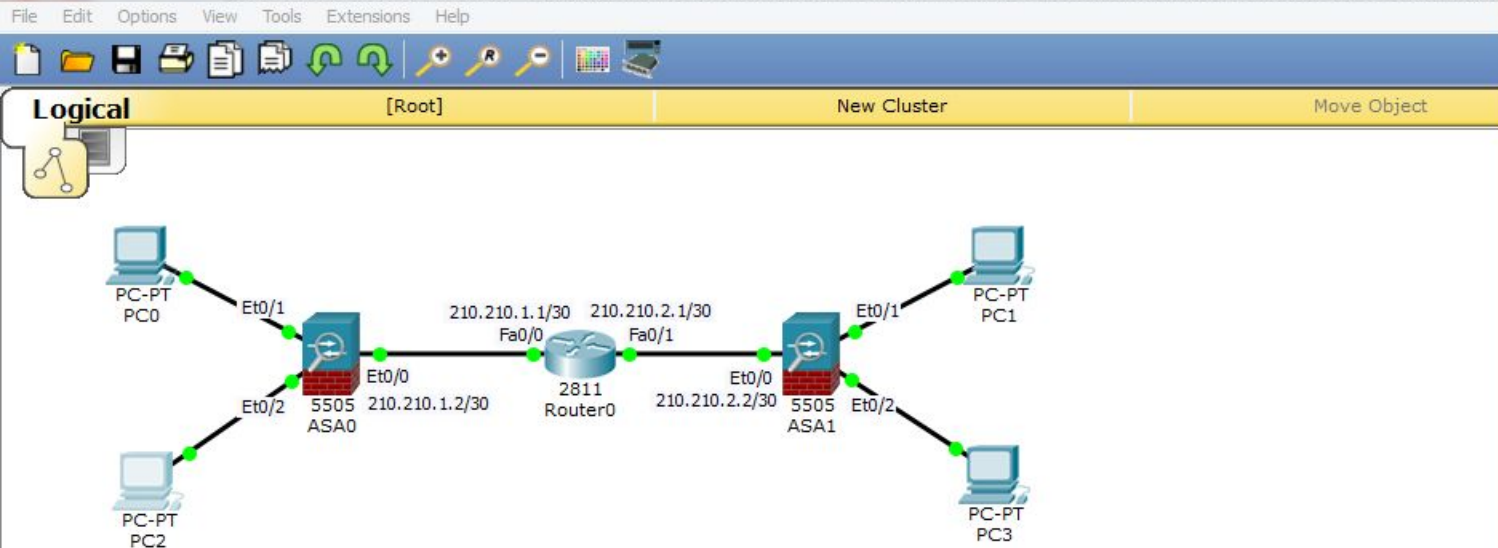
WAN Emulation

Generic Generic DSL Modem Cable Modem

Copper Straight-Through

Scenario 0 New Delete Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
------	-------------	--------	-------------	------	-------	-----------	----------	-----	------	--------



Physical Config Desktop Custom Interface

Command Prompt

```

PC>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=16ms TTL=126
Reply from 192.168.2.6: bytes=32 time=13ms TTL=126
Reply from 192.168.2.6: bytes=32 time=10ms TTL=126
Reply from 192.168.2.6: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 16ms, Average = 13ms

PC>ping 192.168.2.6

Pinging 192.168.2.6 with 32 bytes of data:

Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=10ms TTL=126
Reply from 192.168.2.6: bytes=32 time=11ms TTL=126
Reply from 192.168.2.6: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 11ms, Average = 10ms

PC>

```

В заключении проверим связь между добавленными компьютерами из

Центрального офиса и филиала: «ping 192.168.2.6».

Связь есть!!!

Таким образом мы построили VPN-соединение, используя Cisco ASA!!!

WAN Emulation: Generic, Generic, DSL Modem, Cable Modem

Copper Straight-Through

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
Scenario 0										
New Delete										
Toggle PDU List Window										

Маска подсети	Маска в двоичной системе	Префикс	Количество адресов	Обратная маска
255.255.255.255	11111111.11111111.11111111.11111111	/32	1	0.0.0.0
255.255.255.254	11111111.11111111.11111111.11111110	/31	2	0.0.0.1
255.255.255.252	11111111.11111111.11111111.11111100	/30	4	0.0.0.3
255.255.255.248	11111111.11111111.11111111.11111000	/29	8	0.0.0.7
255.255.255.240	11111111.11111111.11111111.11110000	/28	16	0.0.0.15
255.255.255.224	11111111.11111111.11111111.11100000	/27	32	0.0.0.31
255.255.255.192	11111111.11111111.11111111.11000000	/26	64	0.0.0.63
255.255.255.128	11111111.11111111.11111111.10000000	/25	128	0.0.0.127
255.255.255.0	11111111.11111111.11111111.00000000	/24	256	0.0.0.255
255.255.254.0	11111111.11111111.11111110.00000000	/23	512	0.0.1.255
255.255.252.0	11111111.11111111.11111100.00000000	/22	1024	0.0.3.255
255.255.248.0	11111111.11111111.11111000.00000000	/21	2048	0.0.7.255
255.255.240.0	11111111.11111111.11110000.00000000	/20	4096	0.0.15.255
255.255.224.0	11111111.11111111.11100000.00000000	/19	8192	0.0.31.255
255.255.192.0	11111111.11111111.11000000.00000000	/18	16384	0.0.63.255
255.255.128.0	11111111.11111111.10000000.00000000	/17	32768	0.0.127.255
255.255.0.0	11111111.11111111.00000000.00000000	/16	65536	0.0.255.255
255.254.0.0	11111111.11111110.00000000.00000000	/15	131072	0.1.255.255
255.252.0.0	11111111.11111100.00000000.00000000	/14	262144	0.3.255.255
255.248.0.0	11111111.11111000.00000000.00000000	/13	524288	0.7.255.255
255.240.0.0	11111111.11110000.00000000.00000000	/12	1048576	0.15.255.255

Список литературы:

1. Компьютерные сети. Н.В. Максимов, И.И. Попов, 4-е издание, переработанное и дополненное, «Форум», Москва, 2010.
2. Компьютерные сети. Принципы, технологии, протоколы, В. Олифер, Н. Олифер (5-е издание), «Питер», Москва, Санкт-Петербург, 2016.
3. Компьютерные сети. Э. Таненбаум, 4-е издание, «Питер», Москва, Санкт-Петербург, 2003.

Список ссылок:

<http://blog.netskills.ru/2014/03/firewall-vs-router.html>

<https://drive.google.com/file/d/0B-5kZI7ixcSKS0ZIUHZ5WnhWeVk/view>

Спасибо за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: asoloduhin@kait20.ru