NCY-2
Assignment 2

Abdul Sami Qasim
22i-1725
CY-C

Submitted to: Sir Abdullah Abid

Date of Submission: September 28, 2024

Contents

Introduction

In this assignment, we were told to make a topology involving a pc, a webserver, and a firewall. Afterwards, we were told to configure the firewall in such a way that only ICMP and web traffic can go through.

Tasks

Following are the tasks to complete in this assignment:

- Make a topology consisting of a PC, a cisco ASA 5505 firewall and a server.
- Assign specified IPs to the devices.
- Configure outside and inside ports of the firewall according to given information.
- Setup outside and inside vlan.
- Set gateways.
- Implement NAT on firewall.
- Implement ACL to allow only web and ping traffic.
- Apply ACL on outside interface in inbound direction.
- Generate traffic to see if everything is working.

Making the Topology:

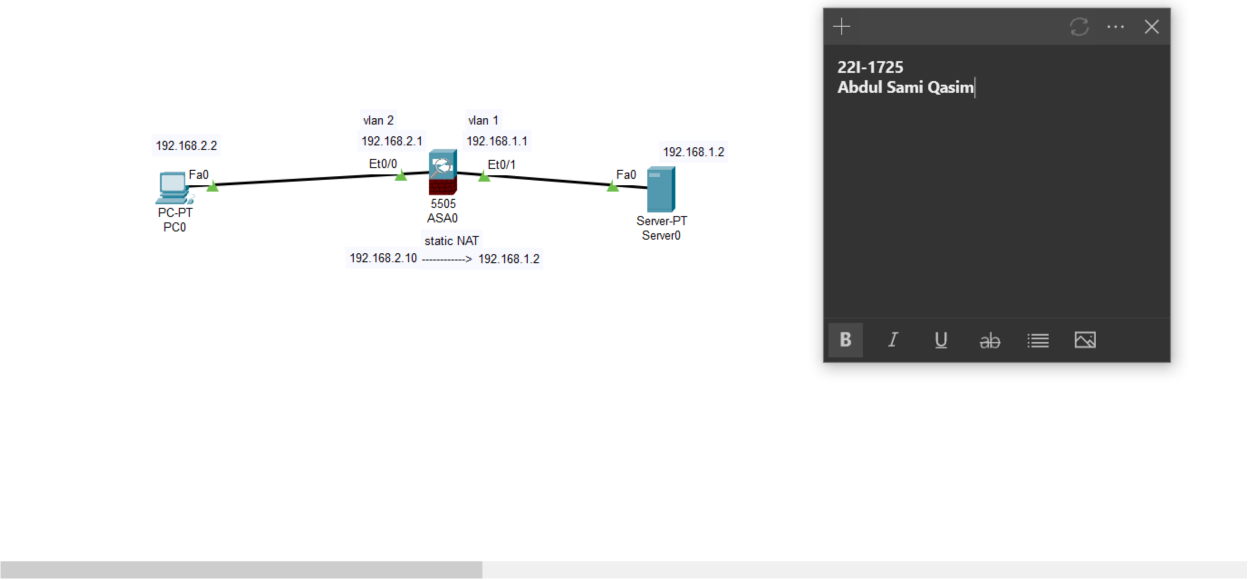
Starting with making the topology, I used the following components:

1. 1x PC
2. 1x Cisco ASA 5505 firewall
3. 1x Web Server

The following table contains the IP configurations of the components in the topology:

Component	IP	Subnet	Gateway
PC0	192.168.2.2	255.255.255.0	192.168.2.1
ASA0 Et0/0	192.168.2.1	255.255.255.0	-
ASA0 Et0/1	192.168.1.1	255.255.255.0	-
Server0	192.168.1.2	255.255.255.0	192.168.1.1

This is the topology I got:

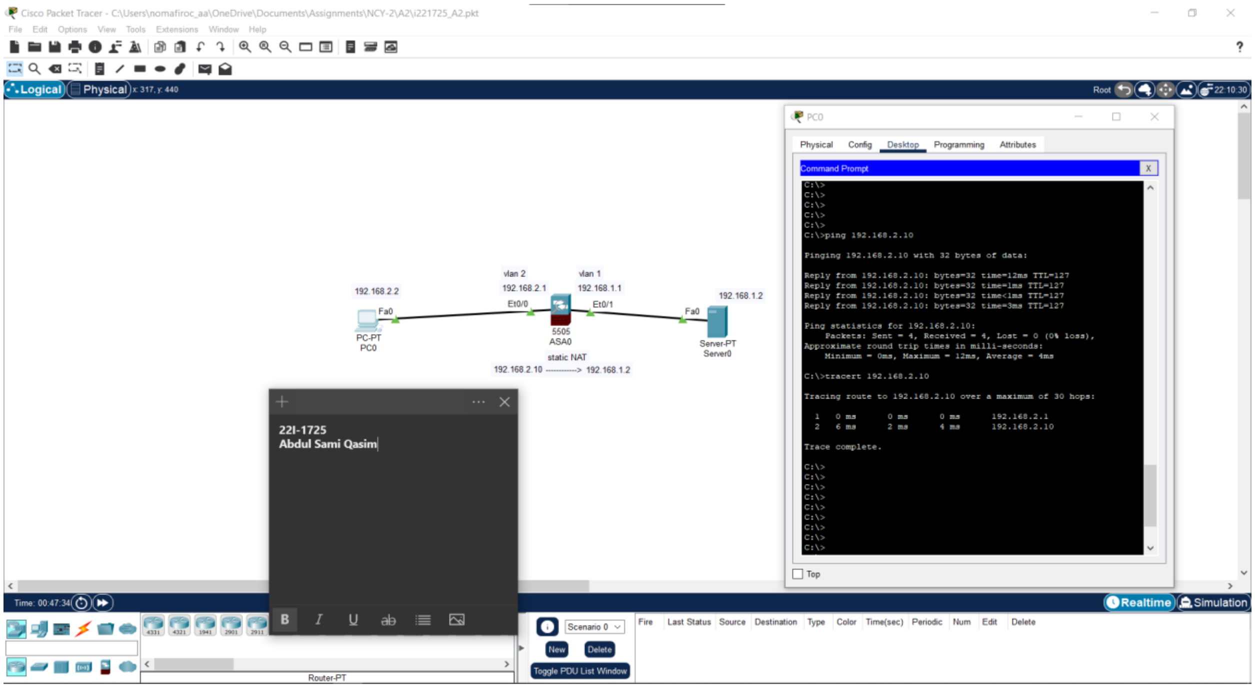


22I-1725
Abdul Sami Qasim

Figure 1: Required Topology

Ping and traceroute:

Pinging the server from the computer and using tracert command to see the full route from pc to server:

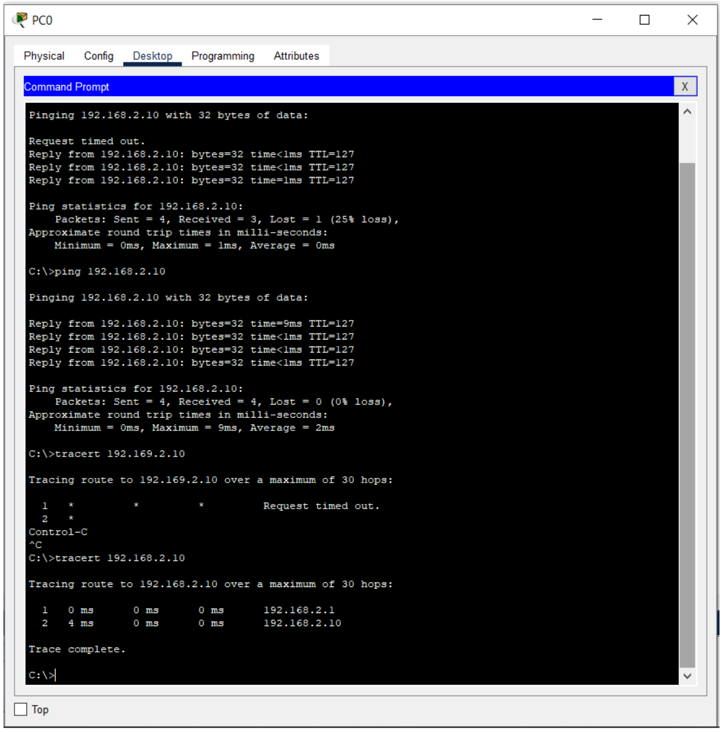


221-1725
Abdul Sami Qasim

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=12ms TTL=127
Reply from 192.168.2.10: bytes=32 time=1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 4ms

C:\>tracert 192.168.2.10

Tracing route to 192.168.2.10 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.2.1
  2   6 ms      2 ms      4 ms      192.168.2.10

Trace complete.

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

Figure 2: Ping and tracert performed on PC0

Zooming in to show the output clearly:

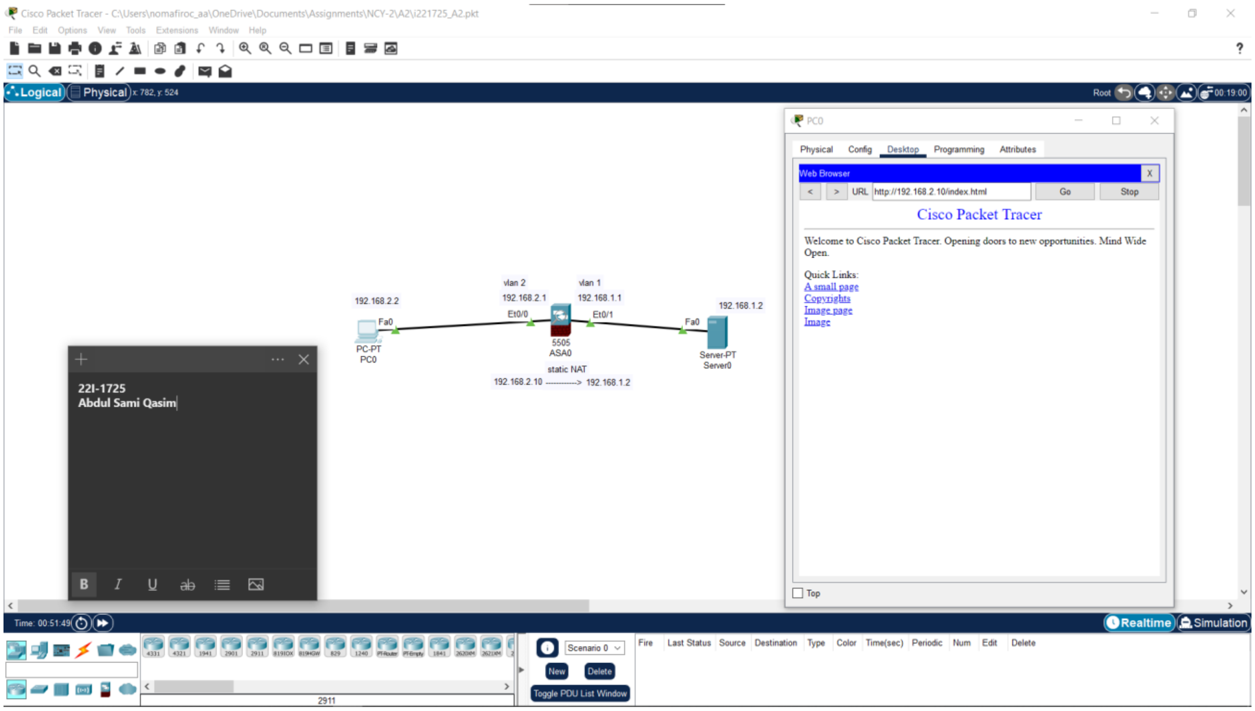


```
Pinging 192.168.2.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=9ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127
Reply from 192.168.2.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>tracert 192.169.2.10

Tracing route to 192.169.2.10 over a maximum of 30 hops:

  1   *         *         *         Request timed out.
  2   *
Control-C
^C
C:\>tracert 192.168.2.10

Tracing route to 192.168.2.10 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.2.1
  2   4 ms      0 ms      0 ms      192.168.2.10

Trace complete.

C:\>
```

Figure 3: Zoomed in output

Web Page Access:

Now accessing the webserver (server0) from PC0



22I-1725
Abdul Sami Qasim

URL: http://192.168.2.10/index.html

Cisco Packet Tracer

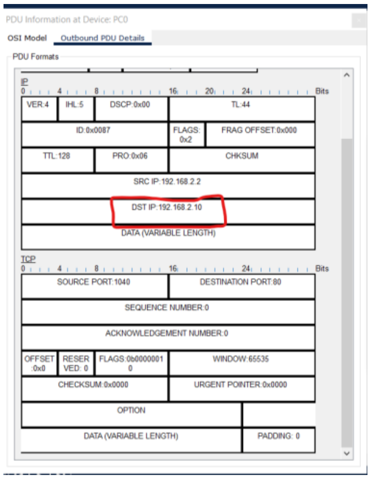
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Figure 4: Accessing the web page on Server0

Traffic from PC to firewall:

Showing the TCP and IP headers of a packet going from PC0 to ASA0. As this is before NAT, it will show the IP I tried to access (192.168.2.10) as the destination IP.



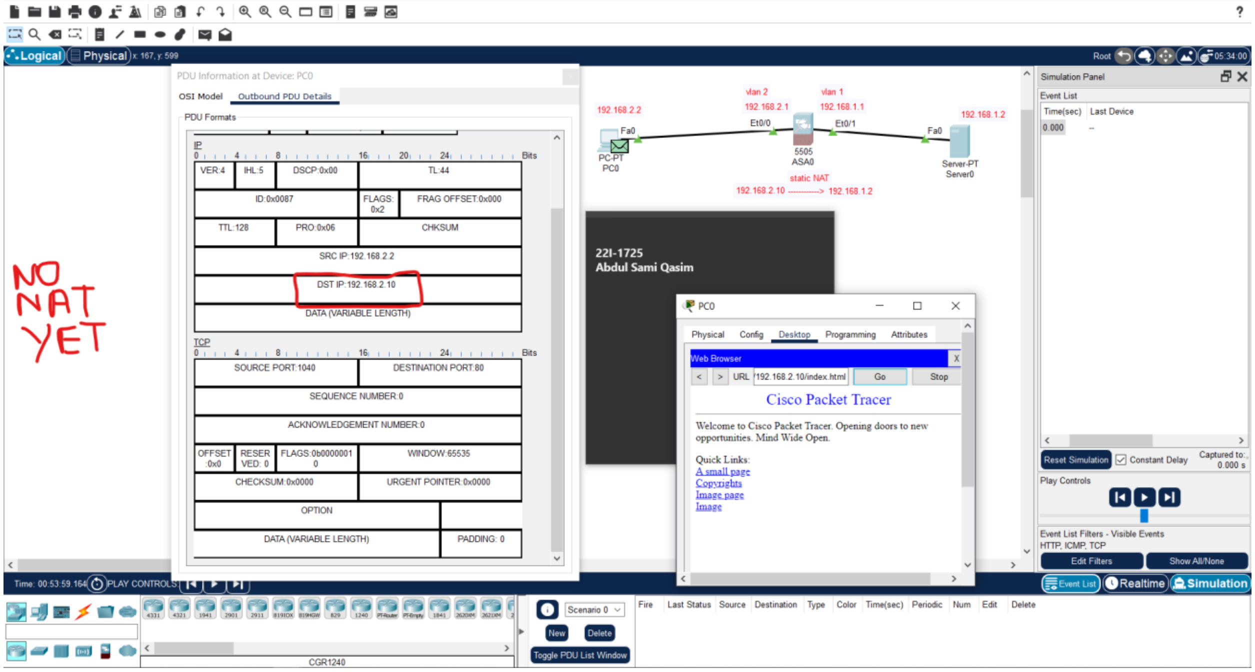
IP

VER:4	IHL:5	DSCP:0x00	TL:44
ID:0x0087		FLAGS: 0x2	FRAG OFFSET:0x000
TTL:128	PRO:0x06	CHKSUM	
SRC IP:192.168.2.2			
DST IP:192.168.2.10			
DATA (VARIABLE LENGTH)			

TCP

SOURCE PORT:1040		DESTINATION PORT:80	
SEQUENCE NUMBER:0			
ACKNOWLEDGEMENT NUMBER:0			
OFFSET :0x0	RESER VED: 0	FLAGS:0b0000001 0	WINDOW:65535
CHECKSUM:0x0000		URGENT POINTER:0x0000	
OPTION			
DATA (VARIABLE LENGTH)			PADDING: 0

Figure 5: PC0 to ASA0 packet headers



NO NAT YET

PDU Information at Device: PC0

OSI Model | Outbound PDU Details

PDU Formats

IP

VER:4 | IHL:5 | DSCP:0x00 | TL:44

ID:0x0087 | FLAGS: 0x2 | FRAG OFFSET:0x000

TTL:128 | PRO:0x06 | CHKSUM

SRC IP:192.168.2.2

DST IP:192.168.2.10

DATA (VARIABLE LENGTH)

TCP

SOURCE PORT:1040 | DESTINATION PORT:80

SEQUENCE NUMBER:0

ACKNOWLEDGEMENT NUMBER:0

OFFSET :0x0 | RESER VED: 0 | FLAGS:0b0000001 0 | WINDOW:65535

CHECKSUM:0x0000 | URGENT POINTER:0x0000

OPTION

DATA (VARIABLE LENGTH) | PADDING: 0

PC0 — Physical | Config | Desktop | Programming | Attributes

Web Browser

URL /192.168.2.10/index.html

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Simulation Panel — Event List

Time(sec)	Last Device
0.000	--

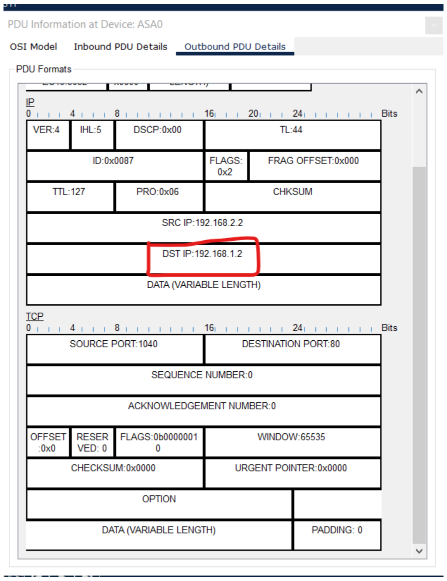
☑ Constant Delay — Captured to: 0.000 s

Event List Filters - Visible Events
HTTP, ICMP, TCP

Figure 6: PC0 to ASA0 packet

Traffic from firewall to web server:

Showing the TCP and IP headers of the packet going from ASA0 to Server0. As NAT has been implemented, the destination IP will now be 192.168.1.2.



PDU Information at Device: ASA0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

IP

VER:4 | IHL:5 | DSCP:0x00 | TL:44

ID:0x0087 | FLAGS: 0x2 | FRAG OFFSET:0x000

TTL:127 | PRO:0x06 | CHKSUM

SRC IP:192.168.2.2

DST IP:192.168.1.2

DATA (VARIABLE LENGTH)

TCP

SOURCE PORT:1040 | DESTINATION PORT:80

SEQUENCE NUMBER:0

ACKNOWLEDGEMENT NUMBER:0

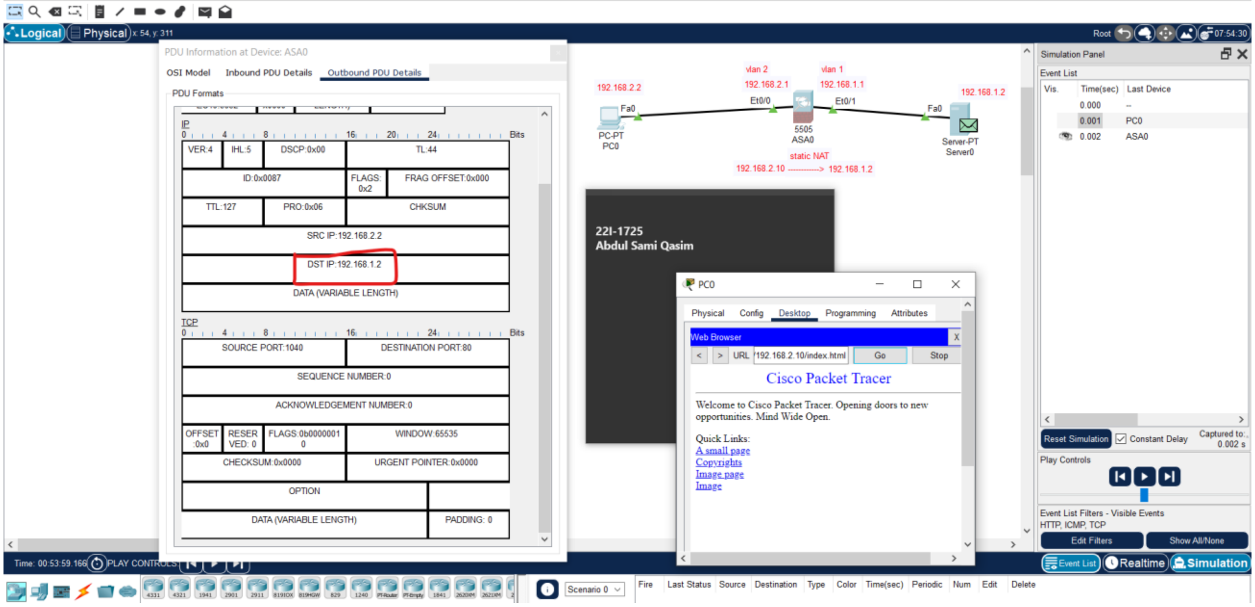
OFFSET :0x0 | RESER VED: 0 | FLAGS:0b0000001 0 | WINDOW:65535

CHECKSUM:0x0000 | URGENT POINTER:0x0000

OPTION

DATA (VARIABLE LENGTH) | PADDING: 0

Figure 7: ASA0 to Server0 packet headers



PDU Information at Device: ASA0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

IP

VER:4 | IHL:5 | DSCP:0x00 | TL:44

ID:0x0087 | FLAGS: 0x2 | FRAG OFFSET:0x000

TTL:127 | PRO:0x06 | CHKSUM

SRC IP:192.168.2.2

DST IP:192.168.1.2

DATA (VARIABLE LENGTH)

TCP

SOURCE PORT:1040 | DESTINATION PORT:80

SEQUENCE NUMBER:0

ACKNOWLEDGEMENT NUMBER:0

OFFSET :0x0 | RESERVED: 0 | FLAGS:0b0000001 0 | WINDOW:65535

CHECKSUM:0x0000 | URGENT POINTER:0x0000

OPTION

DATA (VARIABLE LENGTH) | PADDING: 0

PC0 Web Browser

URL 192.168.2.10/index.html

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

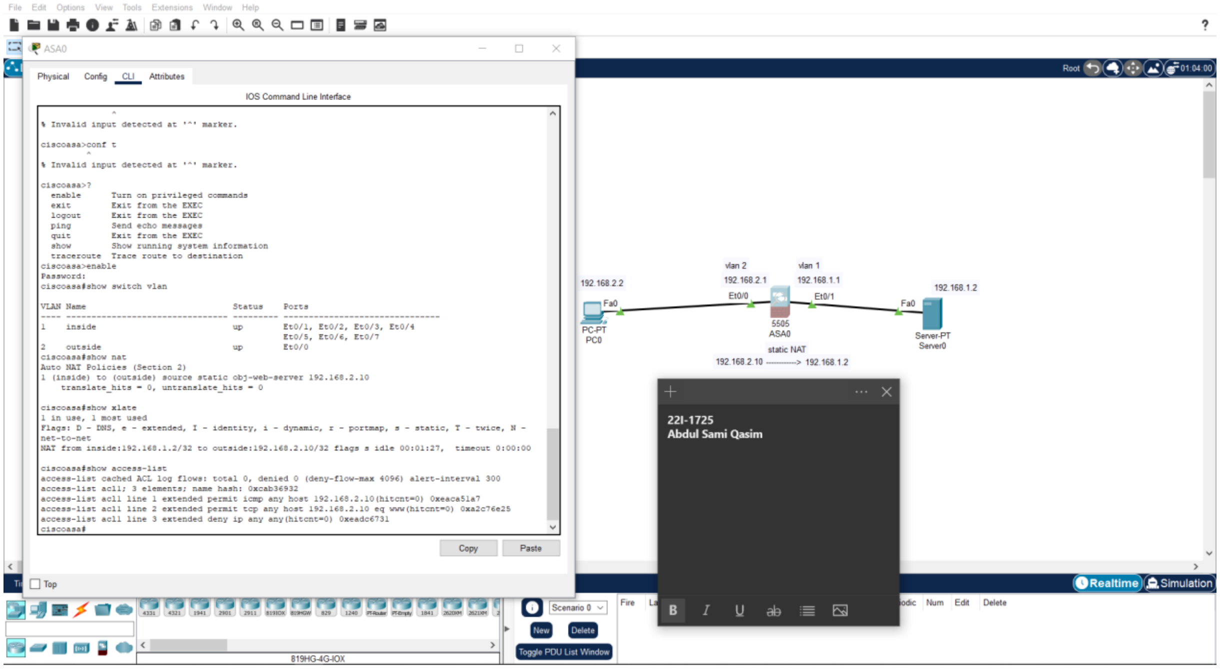
Quick Links:
A small page
Copyrights
Image page
Image

221-1725
Abdul Sami Qasim

Figure 8: ASA0 to Server0 packet

As you can see, the destination IP successfully changed from 192.168.2.10 to 192.168.1.2, therefore the NAT implementation is working as intended.

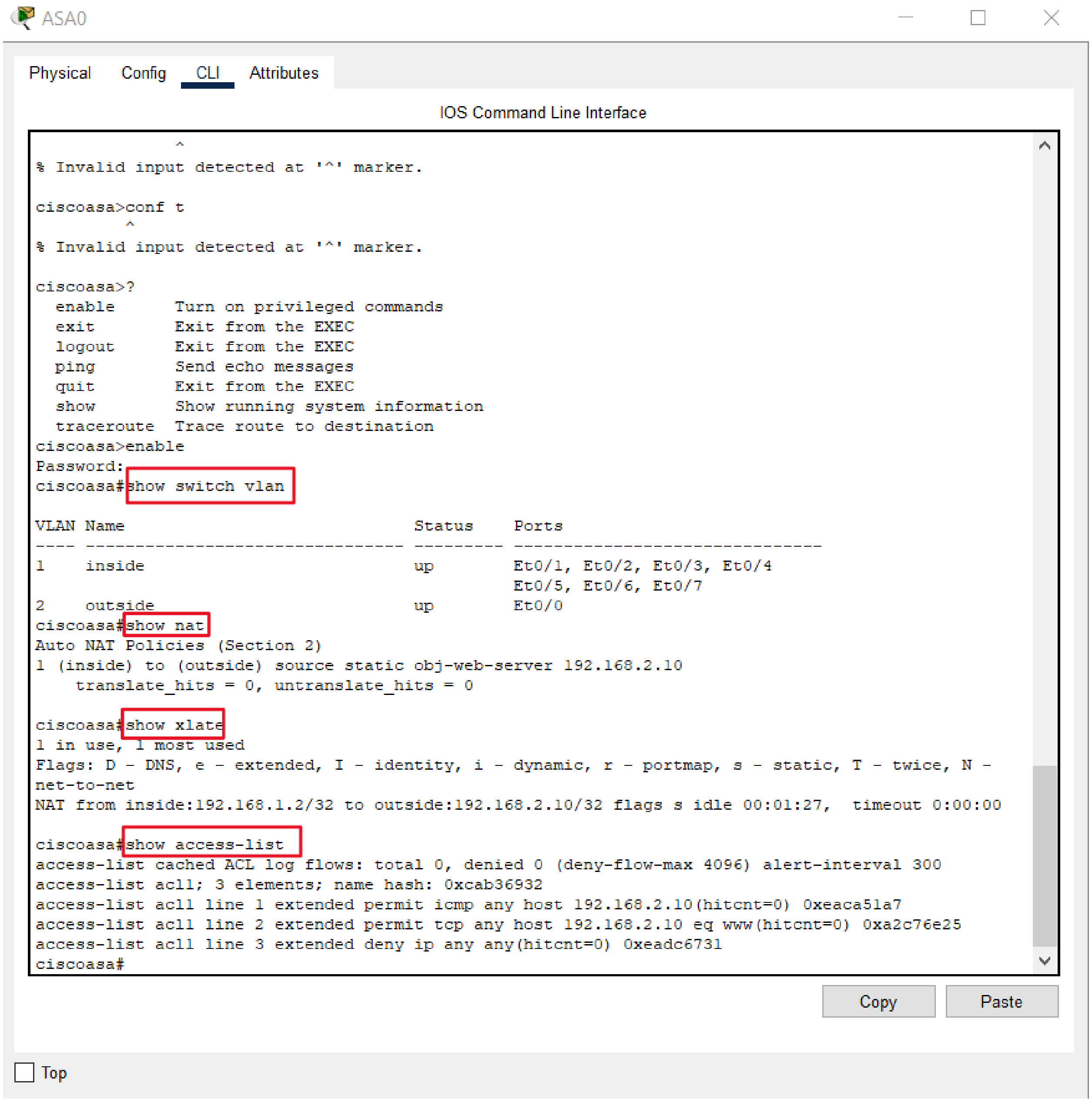
Command Outputs:



```
              ^
% Invalid input detected at '^' marker.

ciscoasa>conf t
          ^
% Invalid input detected at '^' marker.

ciscoasa>?
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  quit        Exit from the EXEC
  show        Show running system information
  traceroute  Trace route to destination
ciscoasa>enable
Password:
ciscoasa#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           up        Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          up        Et0/0
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static obj-web-server 192.168.2.10
    translate_hits = 0, untranslate_hits = 0

ciscoasa#show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T - twice, N -
net-to-net
NAT from inside:192.168.1.2/32 to outside:192.168.2.10/32 flags s idle 00:01:27,  timeout 0:00:00

ciscoasa#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list acl1; 3 elements; name hash: 0xcab36932
access-list acl1 line 1 extended permit icmp any host 192.168.2.10(hitcnt=0) 0xeaca51a7
access-list acl1 line 2 extended permit tcp any host 192.168.2.10 eq www(hitcnt=0) 0xa2c76e25
access-list acl1 line 3 extended deny ip any any(hitcnt=0) 0xeadc6731
ciscoasa#
```

221-1725
Abdul Sami Qasim

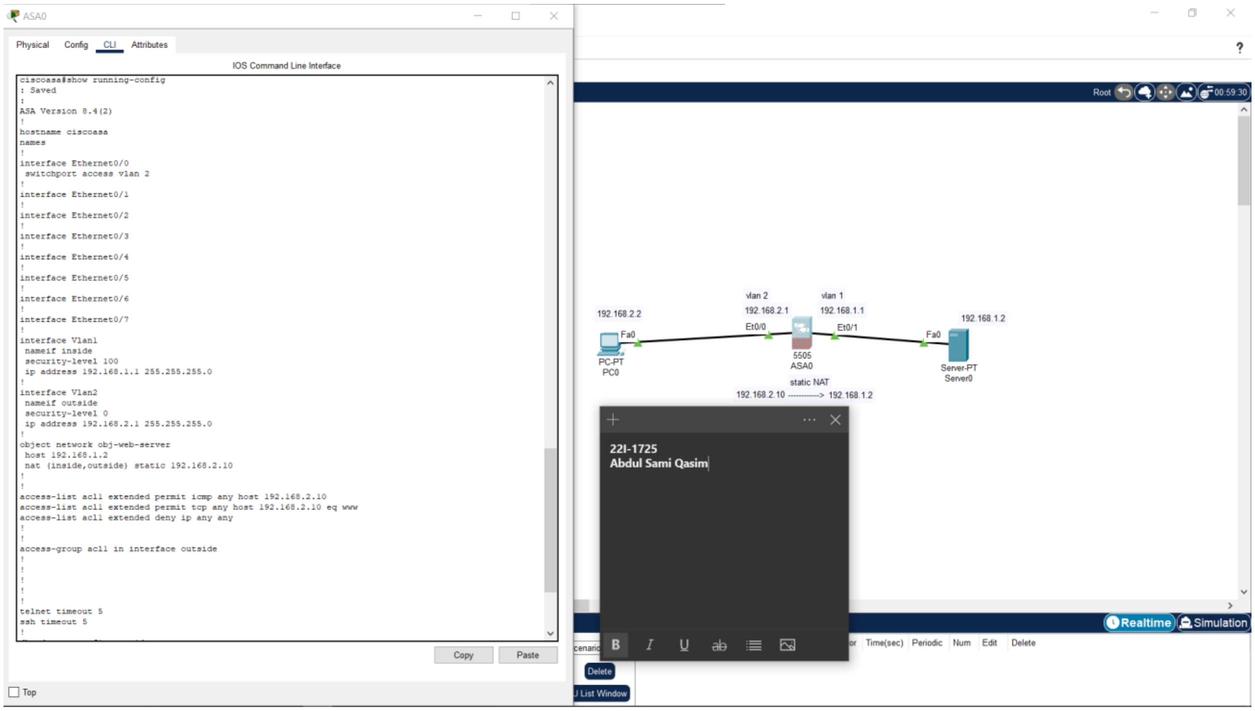
Figure 9: All command outputs



```
              ^
% Invalid input detected at '^' marker.

ciscoasa>conf t
         ^
% Invalid input detected at '^' marker.

ciscoasa>?
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  quit        Exit from the EXEC
  show        Show running system information
  traceroute  Trace route to destination
ciscoasa>enable
Password:
ciscoasa#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           up        Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          up        Et0/0
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source static obj-web-server 192.168.2.10
    translate_hits = 0, untranslate_hits = 0

ciscoasa#show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T - twice, N -
net-to-net
NAT from inside:192.168.1.2/32 to outside:192.168.2.10/32 flags s idle 00:01:27,  timeout 0:00:00

ciscoasa#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list acl1; 3 elements; name hash: 0xcab36932
access-list acl1 line 1 extended permit icmp any host 192.168.2.10(hitcnt=0) 0xeaca51a7
access-list acl1 line 2 extended permit tcp any host 192.168.2.10 eq www(hitcnt=0) 0xa2c76e25
access-list acl1 line 3 extended deny ip any any(hitcnt=0) 0xeadc6731
ciscoasa#
```

Figure 10: Zoomed in command outputs

Output of running-config



```
ciscoasa#show running-config
: Saved
:
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
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.2.1 255.255.255.0
!
object network obj-web-server
 host 192.168.1.2
 nat (inside,outside) static 192.168.2.10
!
!
access-list acl1 extended permit icmp any host 192.168.2.10
access-list acl1 extended permit tcp any host 192.168.2.10 eq www
access-list acl1 extended deny ip any any
!
!
access-group acl1 in interface outside
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
```

Figure 11: running-config

Copy pasted output of running-config:

```
ciscoasa#show running-config
: Saved
:
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
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.2.1 255.255.255.0
!
object network obj-web-server
 host 192.168.1.2
 nat (inside,outside) static 192.168.2.10
!
!
access-list acl1 extended permit icmp any host 192.168.2.10
access-list acl1 extended permit tcp any host 192.168.2.10 eq www
access-list acl1 extended deny ip any any
!
!
access-group acl1 in interface outside
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
!
!
!
!
```