# Task 47

# INE LABS Section 1 - TASK 1 - ASA NAT AND PAT

CYBERNET

Total Quality Network

**Submitted by: Shair Khan**

**Submitted to: Sir Ismail Khan**

**Designation: TAC Engineer Level 1**

This task involves three NAT scenarios — PAT on ASA, Dynamic NAT on ASA with fallback behavior when IP pools are exhausted.

## 1. What is NAT and why use it here?

- **NAT (Network Address Translation)** translates private IP addresses (inside network) into public IP addresses (outside network) so that hosts can communicate over the internet.
- In this task:
    - **Dynamic NAT** is used when you have a pool of public IPs, and inside hosts get mapped to them dynamically.
    - **PAT (Port Address Translation)** is used when many inside hosts share one public IP address (the ASA's outside IP or a specified IP).
- NAT ensures:
    - Private networks remain hidden from outside.
    - Public IP address usage is optimized.
    - Communication to external services (like `www.ine.com`) is possible.

## 2. First Requirement – PAT for All Inside Hosts on ASA

All hosts behind the inside interface of ASA use PAT with ASA's outside IP.

- This is overload PAT, where multiple inside hosts share the ASA's outside interface IP.
- This is the fallback translation for all inside hosts when no specific NAT pool applies.
- This appears in Section 3 of the `show nat` command because ASA NAT rules are sectioned:
    1. Manual NAT (Section 1)
    2. Auto NAT (Section 2)
    3. After-auto NAT (Section 3)

## 3. Second Requirement – Dynamic NAT with Fallback to PAT on ASA

Inside network 10.0.0.0/24 → NAT pool 120.0.0.102 – 120.0.0.103, fallback to PAT on ASA's outside IP.

- If there are only two public IPs in the pool, only two hosts can have 1:1 mapping at a time.
- If more hosts try to connect, the ASA should automatically use PAT on its outside IP for the rest.
- This ensures:
    - Preferred use of Dynamic NAT (public IP pool).
    - No communication failure when pool is exhausted (fallback to PAT).

## 4. Third Requirement – Dynamic NAT + PAT on Router R1

Create Loopback 0 (10.1.1.0/24) and translate it to pool 120.0.0.202 – 120.0.0.203, fallback to PAT 120.0.0.204.

- R1's Loopback 0 simulates another inside network behind R1.
- NAT pool has two IPs, so only two hosts get 1:1 mapping at a time.
- If more hosts connect, they share 120.0.0.204 using PAT.
- This is dynamic NAT with fallback PAT on a router instead of ASA.

## 5. NAT Global Configuration Requirement

Must appear in Section 1 of `show nat` unless stated otherwise.

- On ASA, NAT rules have **sections**:
  - **Section 1 (Manual NAT / Twice NAT)** → takes priority over everything.
  - **Section 2 (Auto NAT)** → object NAT rules.
  - **Section 3 (After-auto NAT)** → catch-all rules like general PAT.
- The task says global NAT for all requirements (except where they want it in Section 3), meaning we write rules so that they're seen in Section 1 for higher priority.

## 6. Access Requirement

All inside networks must access `www.ine.com` on port **80/443**.

- Port 80 = HTTP, Port 443 = HTTPS.
- After NAT, ASA must allow traffic to these ports (ACL configuration).
- This tests NAT and firewall policy working together.

## Logical Flow of Translation

1. Packet from inside host → ASA checks NAT rules in order:
   - If source is 10.0.0.0/24, try Dynamic NAT pool (120.0.0.102–103).
   - If pool exhausted, fall back to PAT (ASA outside IP).
2. Packet from R1 Loopback → NAT pool (120.0.0.202–203).
   - If pool exhausted, PAT with 120.0.0.204.
3. All other traffic uses PAT with ASA outside IP.
4. ASA ACL permits HTTP/HTTPS to www.ine.com.

## Key ASA & Router NAT Concepts for This Task

- **Dynamic NAT** = many-to-many mapping (uses a pool, 1:1 per connection).
- **PAT (Overload)** = many-to-one mapping using different port numbers.
- **NAT Order in ASA** = Section 1 → Section 2 → Section 3.
- **Fallback** = Configure NAT rules so that if pool is full, PAT takes over automatically.

| Feature | Static NAT | Dynamic NAT | PAT (Port Address Translation) |
|---|---|---|---|
| **Mapping Type** | One-to-one **fixed** mapping between private IP and public IP. | One-to-one **temporary** mapping between private IP and a public IP from a pool. | Many-to-one mapping; multiple private IPs share one public IP (different ports used). |
| **IP Address Assignment** | Always the same public IP for the same internal host. | First-come, first-served from the pool; changes each session. | All internal hosts share the same public IP or a small set of IPs. |
| **Public IP Requirement** | Needs **one public IP per host**. | Needs a **pool of public IPs** (smaller than or equal to number of hosts). | Needs **only one public IP** for all hosts (or very few). |
| **Address Consistency** | Public IP stays constant for that host. | Public IP changes based on pool availability. | Public IP is the same for all; ports make them unique. |
| **Typical Use Case** | Hosting a server (web, email) that must be reachable from outside with a fixed address. | Allowing multiple internal hosts access to outside, but with unique public IPs temporarily. | Most common for internet access when public IPs are scarce. |
| **Configuration Complexity** | Simple; map single inside IP to single outside IP. | Slightly more complex; define inside pool and match traffic. | Simple; usually just "overload" or "PAT" command. |
| **Security** | Least secure (outside always knows which inside host is tied to the IP). | More secure than static because mapping is temporary. | Most secure from IP perspective, since many hosts hide behind one IP. |
| **NAT Example** | `static (inside,outside) 203.0.113.10 192.168.1.10` | Pool 203.0.113.20–30 for inside 192.168.1.0/24 | `nat (inside,outside) after-auto source dynamic any interface` |
| **Impact if Pool Exhausted** | Not applicable (1:1 fixed). | Additional hosts cannot get outside access unless PAT fallback configured. | No pool exhaustion — many can share. |

## NAT Sections in Cisco ASA

When you run `show nat` on an ASA, NAT rules are displayed in three main sections. The section determines priority and order of evaluation.

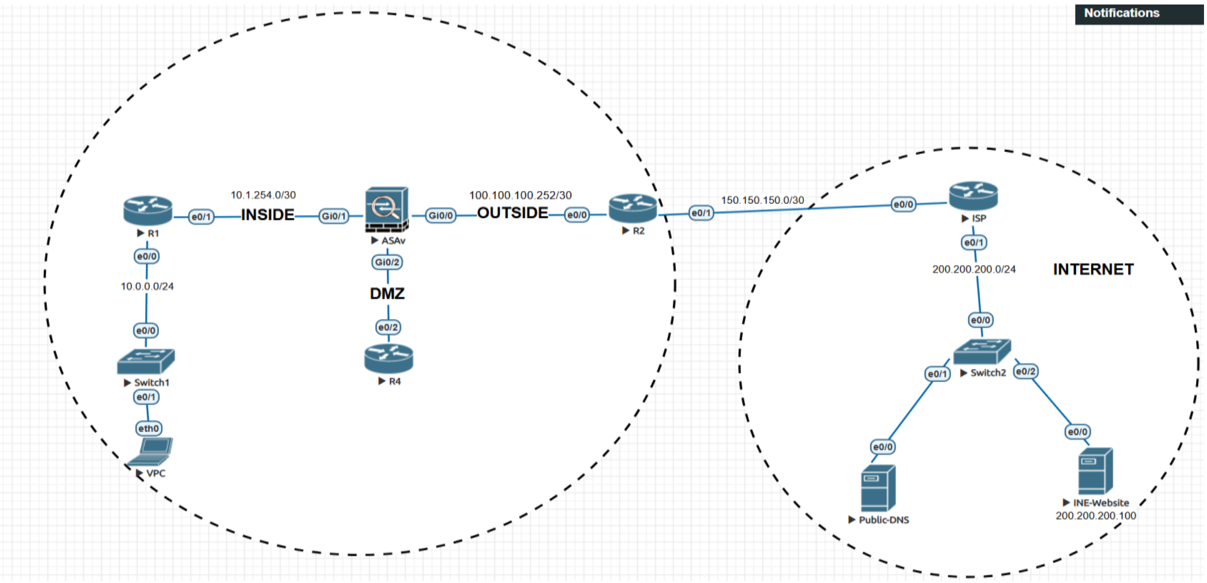
| Section | Type of NAT | Also Called | Priority | Key Points | Example Usage |
|---|---|---|---|---|---|
| **Section 1** | **Manual NAT / Twice NAT** | Policy NAT | Highest | - Applied **before routing lookup**.<br>- Can match both **source** and **destination**.<br>- Used for advanced NAT scenarios like VPN NAT, selective NAT based on destination, or dual NAT. | - NAT only when going to a specific outside network.<br>- Translate 10.0.0.5 to 203.0.113.5 **only** when going to 198.51.100.0/24. |
| **Section 2** | **Auto NAT / Object NAT** | Network Object NAT | Medium | - Defined **inside a network object**.<br>- Translates source address only (destination cannot be matched).<br>- Easier to configure but less flexible. | - Translate 10.0.0.0/24 to public pool. |
| **Section 3** | **After-auto NAT / Manual NAT after Auto** | Catch-all NAT | Lowest | - Applied **after routing lookup**.<br>- Used for fallback rules like PAT to interface IP.<br>- Often used for default internet access for all inside hosts. | - PAT all inside networks to ASA outside interface IP if no other NAT rule matched. |

## How it works in processing

When a packet arrives on ASA:

1. **Section 1** rules are checked first (manual/twice NAT).
2. If no match, **Section 2** rules are checked (object NAT).
3. If still no match, **Section 3** rules are checked (after-auto NAT, usually PAT).

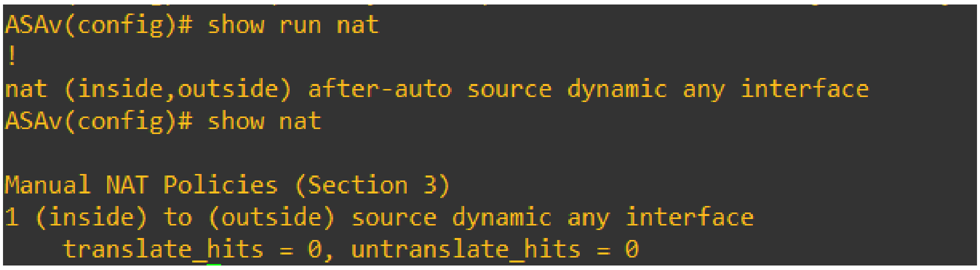
**Network Topology:**



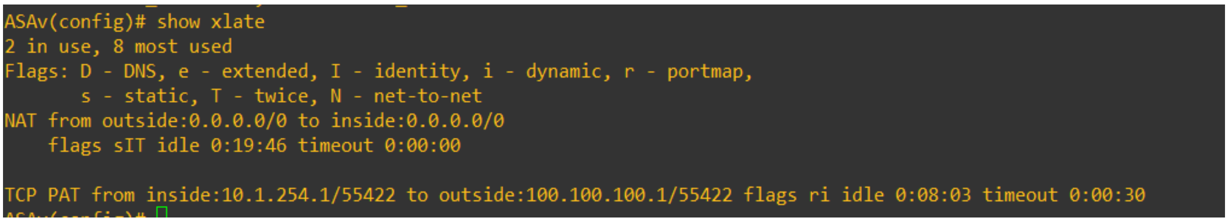
## Task 1.1:

### Configure Dynamic NAT and PAT as per the following requirements:

- All hosts behind the inside interface of ASA, have their addresses PAT translated using the outside IP address of the ASA. This rule must appear in Section 3 when you use the "show nat" command.

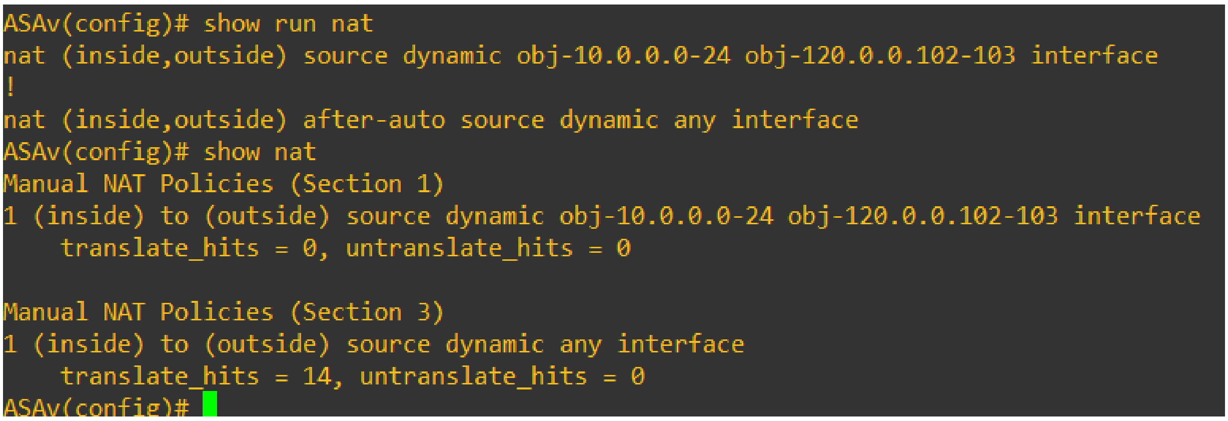


```
ASAv(config)# show run nat
!
nat (inside,outside) after-auto source dynamic any interface
ASAv(config)# show nat

Manual NAT Policies (Section 3)
1 (inside) to (outside) source dynamic any interface
    translate_hits = 0, untranslate_hits = 0
```



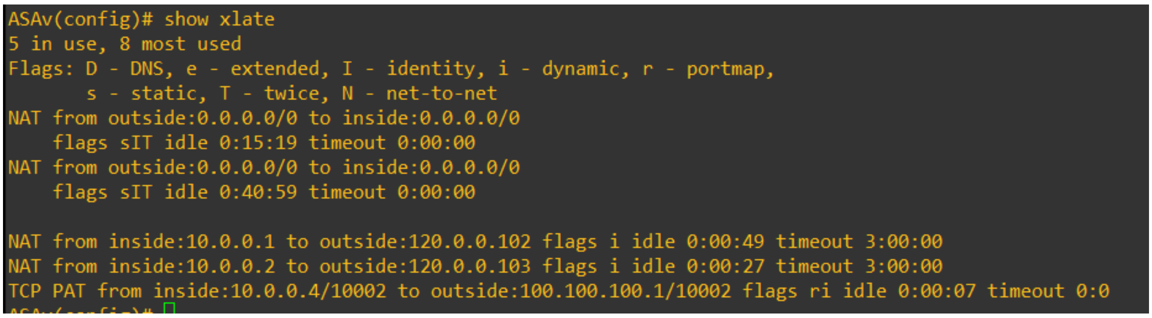
```
ASAv(config)# show xlate
2 in use, 8 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 0:19:46 timeout 0:00:00

TCP PAT from inside:10.1.254.1/55422 to outside:100.100.100.1/55422 flags ri idle 0:08:03 timeout 0:00:30
```

- Configure NAT such that hosts on the inside network 10.0.0.0/24 going to any destination on the outside, have their addresses dynamically translated into an address pool ranging from 120.0.0.102 - 120.0.0.103. If the pool gets exhausted, then they should be dynamically PAT translated using the outside IP address of the ASA.



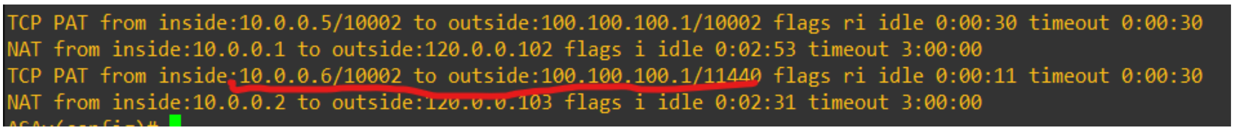
```
ASAv(config)# show run nat
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
!
nat (inside,outside) after-auto source dynamic any interface
ASAv(config)# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
    translate_hits = 0, untranslate_hits = 0

Manual NAT Policies (Section 3)
1 (inside) to (outside) source dynamic any interface
    translate_hits = 14, untranslate_hits = 0
ASAv(config)#
```

NAT and PAT within the range of IP:



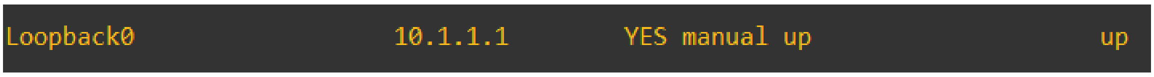
```
ASAv(config)# show xlate
5 in use, 8 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 0:15:19 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 0:40:59 timeout 0:00:00

NAT from inside:10.0.0.1 to outside:120.0.0.102 flags i idle 0:00:49 timeout 3:00:00
NAT from inside:10.0.0.2 to outside:120.0.0.103 flags i idle 0:00:27 timeout 3:00:00
TCP PAT from inside:10.0.0.4/10002 to outside:100.100.100.1/10002 flags ri idle 0:00:07 timeout 0:0
ASAv(config)#
```

After Range is complete, port changed from 100.100.100.1/10002 to 100.100.100.1/ 11400.

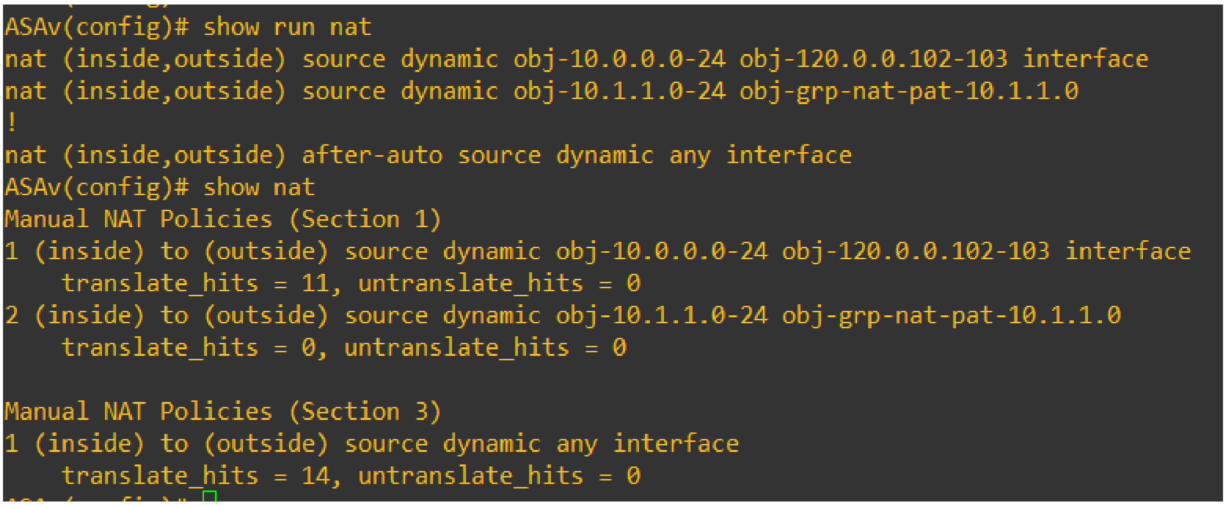


```
TCP PAT from inside:10.0.0.5/10002 to outside:100.100.100.1/10002 flags ri idle 0:00:30 timeout 0:00:30
NAT from inside:10.0.0.1 to outside:120.0.0.102 flags i idle 0:02:53 timeout 3:00:00
TCP PAT from inside:10.0.0.6/10002 to outside:100.100.100.1/11440 flags ri idle 0:00:11 timeout 0:00:30
NAT from inside:10.0.0.2 to outside:120.0.0.103 flags i idle 0:02:31 timeout 3:00:00
ASAv(config)#
```

- Create a new Loopback 0 interface (10.1.1.0/24) on R1. Configure NAT such that hosts on the inside network 10.1.1.0/24 going to any destination on the outside, have their addresses dynamically translated into an address pool ranging from 120.0.0.202 - 120.0.0.203. If the pool gets exhausted, then they should be dynamically PAT translated using the IP address 120.0.0.204.

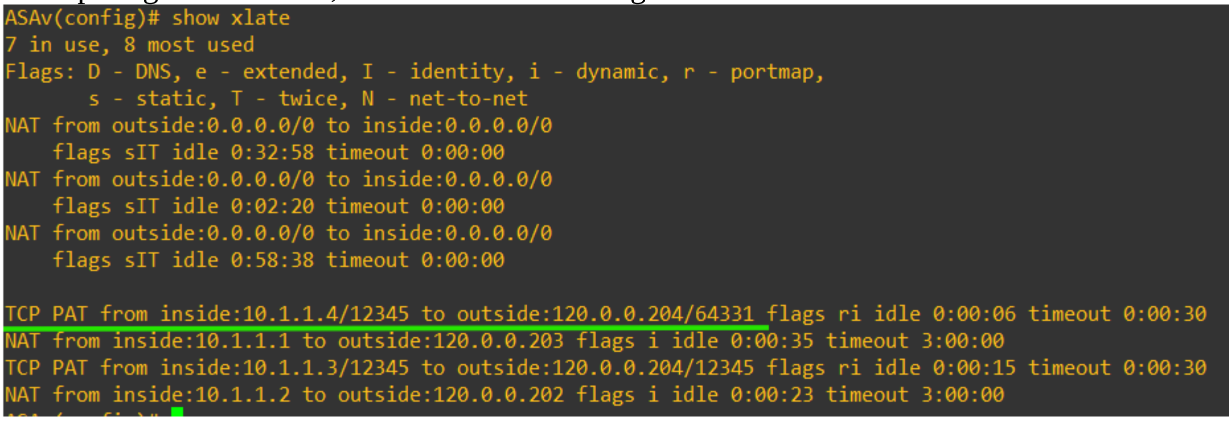


```
Loopback0                  10.1.1.1        YES manual up                    up
```

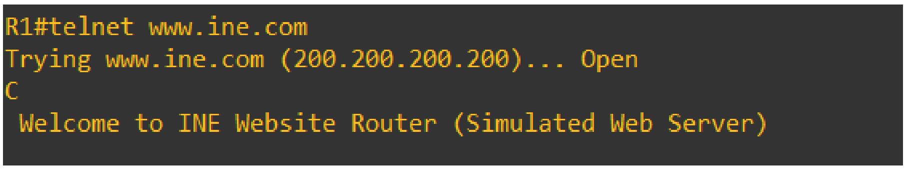


```
ASAv(config)# show run nat
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
nat (inside,outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
!
nat (inside,outside) after-auto source dynamic any interface
ASAv(config)# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
    translate_hits = 11, untranslate_hits = 0
2 (inside) to (outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
    translate_hits = 0, untranslate_hits = 0

Manual NAT Policies (Section 3)
1 (inside) to (outside) source dynamic any interface
    translate_hits = 14, untranslate_hits = 0
```

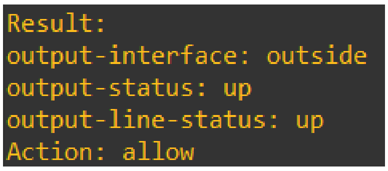
After pool gets exhausted, PAT is translated using IP 120.0.0.204.



```
ASAv(config)# show xlate
7 in use, 8 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 0:32:58 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 0:02:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 0:58:38 timeout 0:00:00

TCP PAT from inside:10.1.1.4/12345 to outside:120.0.0.204/64331 flags ri idle 0:00:06 timeout 0:00:30
NAT from inside:10.1.1.1 to outside:120.0.0.203 flags i idle 0:00:35 timeout 3:00:00
TCP PAT from inside:10.1.1.3/12345 to outside:120.0.0.204/12345 flags ri idle 0:00:15 timeout 0:00:30
NAT from inside:10.1.1.2 to outside:120.0.0.202 flags i idle 0:00:23 timeout 3:00:00
```

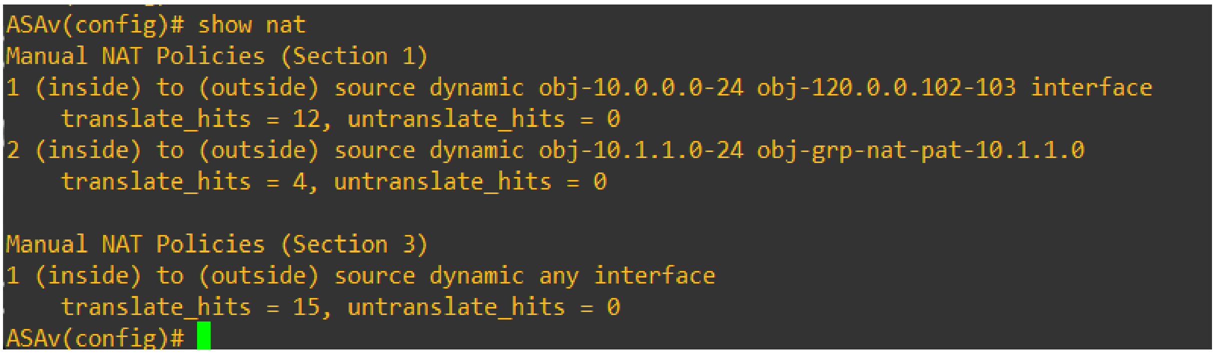


```
R1#telnet www.ine.com
Trying www.ine.com (200.200.200.200)... Open
C
 Welcome to INE Website Router (Simulated Web Server)
```



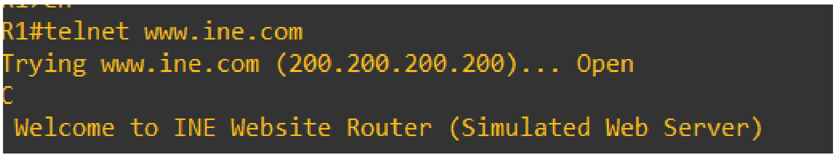
```
Result:
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

- For all these requirements, you must configure NAT globally, which must appear in Section 1 when you use the "show nat" command unless stated otherwise.



```
ASAv(config)# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
    translate_hits = 12, untranslate_hits = 0
2 (inside) to (outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
    translate_hits = 4, untranslate_hits = 0

Manual NAT Policies (Section 3)
1 (inside) to (outside) source dynamic any interface
    translate_hits = 15, untranslate_hits = 0
ASAv(config)#
```

- ❖ All inside networks must be able to access www.ine.com.

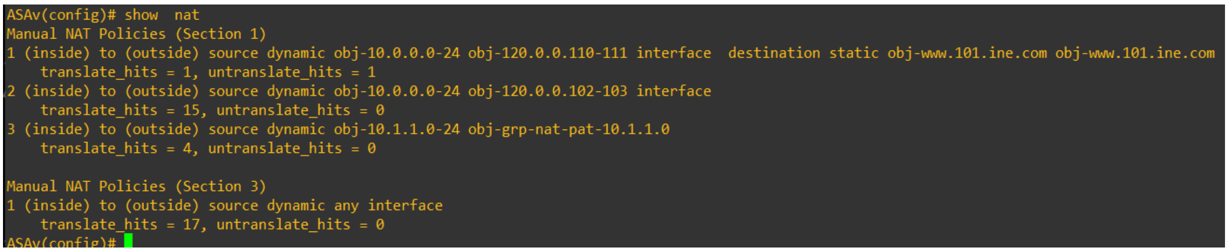


```
R1#telnet www.ine.com
Trying www.ine.com (200.200.200.200)... Open
C
 Welcome to INE Website Router (Simulated Web Server)
```

## Task 1.2

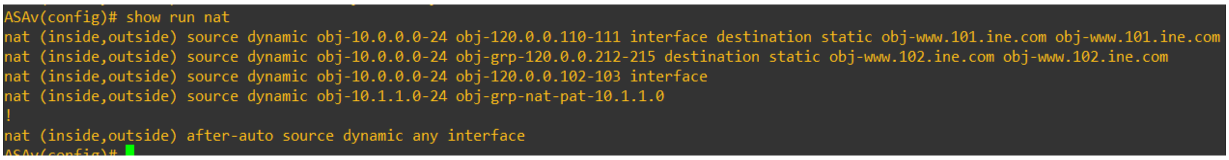
- **Configure Dynamic Policy NAT and PAT as per the following requirements:**

- ❖ Configure NAT such that hosts on the inside network 10.0.0.0/24 going to www.101.ine.com on the outside, have their addresses dynamically translated into an address pool ranging from 120.0.0.110 - 120.0.0.111. If the pool gets exhausted, then they should be dynamically PAT translated using the outside IP address of the ASA.



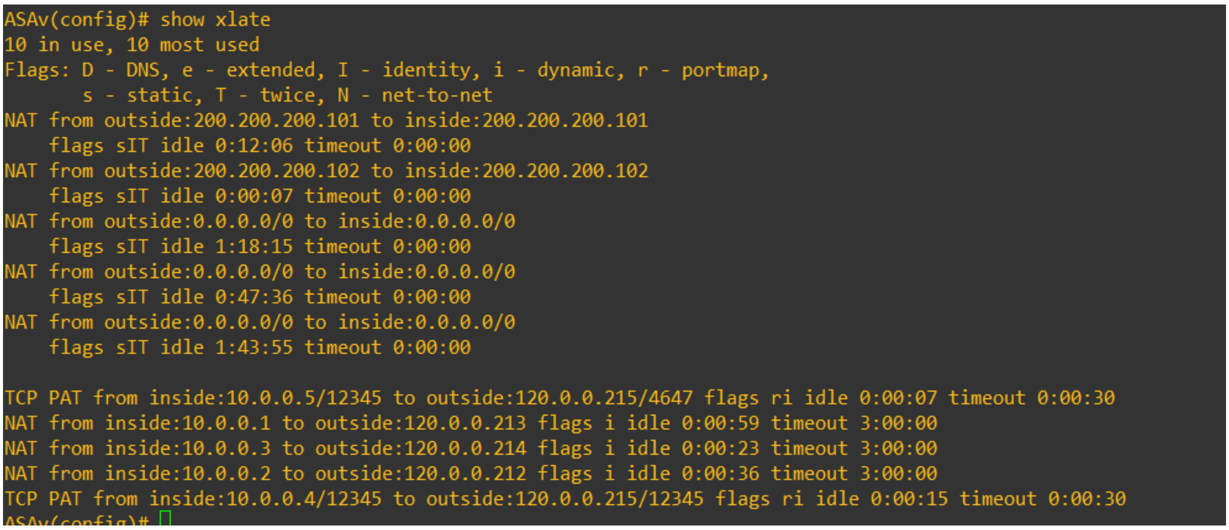
```
ASAv(config)# show  nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.110-111 interface  destination static obj-www.101.ine.com obj-www.101.ine.com
    translate_hits = 1, untranslate_hits = 1
2 (inside) to (outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
    translate_hits = 15, untranslate_hits = 0
3 (inside) to (outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
    translate_hits = 4, untranslate_hits = 0

Manual NAT Policies (Section 3)
1 (inside) to (outside) source dynamic any interface
    translate_hits = 17, untranslate_hits = 0
ASAv(config)#
```

- ❖ Configure NAT such that hosts on the inside network 10.0.0.0/24 going to www.102.ine.com on the outside, have their addresses dynamically translated into an address pool ranging from 120.0.0.212 - 120.0.0.214. If the pool gets exhausted, then they should be dynamically PAT translated using the IP address 120.0.0.215.



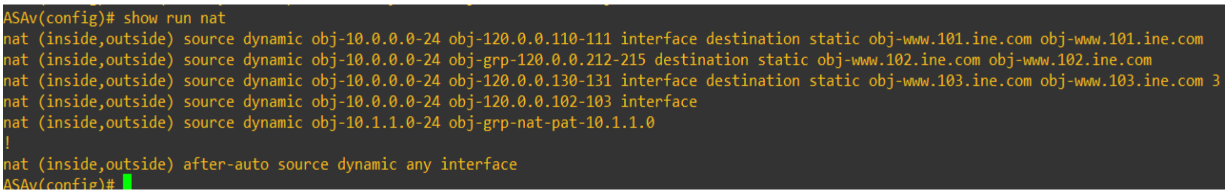
```
ASAv(config)# show run nat
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.110-111 interface destination static obj-www.101.ine.com obj-www.101.ine.com
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-grp-120.0.0.212-215 destination static obj-www.102.ine.com obj-www.102.ine.com
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
nat (inside,outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
!
nat (inside,outside) after-auto source dynamic any interface
ASAv(config)#
```

After pool gets exhausted, it is dynamically PAT translated using the IP address 120.0.0.215

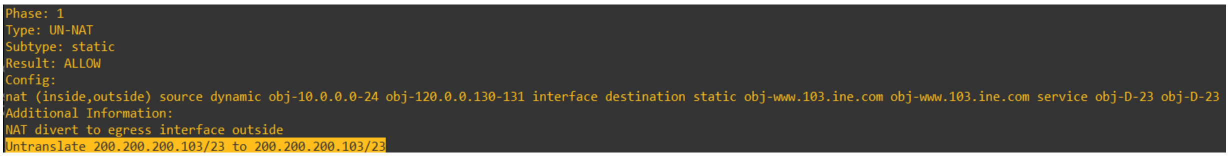


```
ASAv(config)# show xlate
10 in use, 10 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from outside:200.200.200.101 to inside:200.200.200.101
    flags sIT idle 0:12:06 timeout 0:00:00
NAT from outside:200.200.200.102 to inside:200.200.200.102
    flags sIT idle 0:00:07 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 1:18:15 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 0:47:36 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
    flags sIT idle 1:43:55 timeout 0:00:00

TCP PAT from inside:10.0.0.5/12345 to outside:120.0.0.215/4647 flags ri idle 0:00:07 timeout 0:00:30
NAT from inside:10.0.0.1 to outside:120.0.0.213 flags i idle 0:00:59 timeout 3:00:00
NAT from inside:10.0.0.3 to outside:120.0.0.214 flags i idle 0:00:23 timeout 3:00:00
NAT from inside:10.0.0.2 to outside:120.0.0.212 flags i idle 0:00:36 timeout 3:00:00
TCP PAT from inside:10.0.0.4/12345 to outside:120.0.0.215/12345 flags ri idle 0:00:15 timeout 0:00:30
ASAv(config)#
```

❖ TELNET from inside subnet 10.0.0.0/24 to www.103.ine.com should be dynamically translated into an address pool ranging from 120.0.0.130 - 120.0.0.131. If the pool gets exhausted, then they should be dynamically PAT translated using the outside IP address of the ASA.

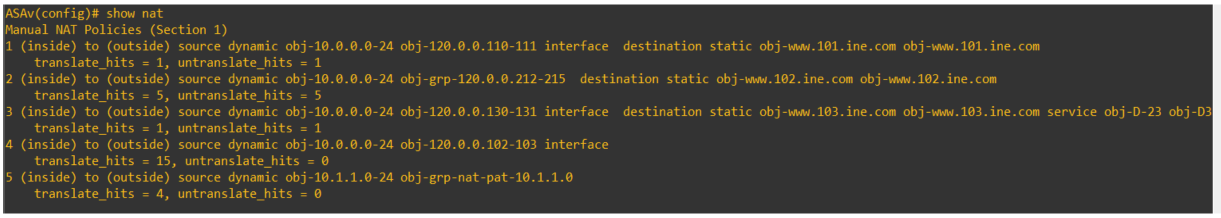


```
ASAv(config)# show run nat
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.110-111 interface destination static obj-www.101.ine.com obj-www.101.ine.com
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-grp-120.0.0.212-215 destination static obj-www.102.ine.com obj-www.102.ine.com
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.130-131 interface destination static obj-www.103.ine.com obj-www.103.ine.com 3
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
nat (inside,outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
!
nat (inside,outside) after-auto source dynamic any interface
ASAv(config)#
```



```
Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.130-131 interface destination static obj-www.103.ine.com obj-www.103.ine.com service obj-D-23 obj-D-23
Additional Information:
NAT divert to egress interface outside
Untranslate 200.200.200.103/23 to 200.200.200.103/23
```

❖ For all these requirements, you must configure NAT globally, which must appear in Section 1 when you use the "show NAT" command.

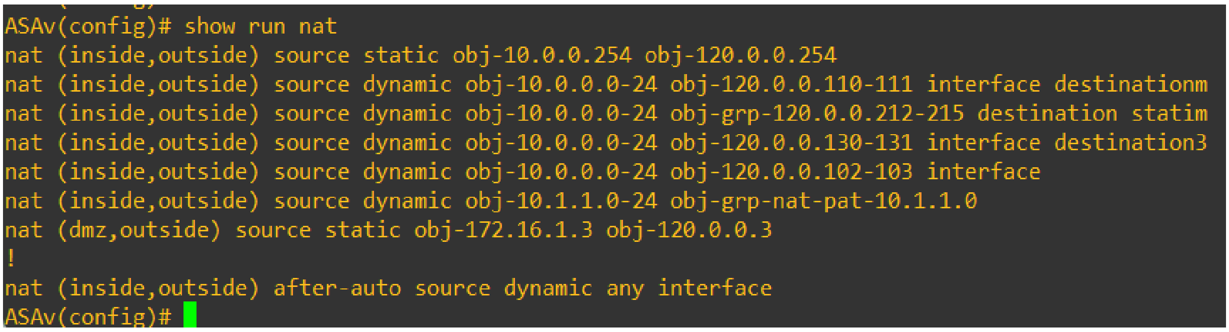


```
ASAv(config)# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.110-111 interface  destination static obj-www.101.ine.com obj-www.101.ine.com
    translate_hits = 1, untranslate_hits = 1
2 (inside) to (outside) source dynamic obj-10.0.0.0-24 obj-grp-120.0.0.212-215  destination static obj-www.102.ine.com obj-www.102.ine.com
    translate_hits = 5, untranslate_hits = 5
3 (inside) to (outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.130-131 interface  destination static obj-www.103.ine.com obj-www.103.ine.com service obj-D-23 obj-D3
    translate_hits = 1, untranslate_hits = 1
4 (inside) to (outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
    translate_hits = 15, untranslate_hits = 0
5 (inside) to (outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
    translate_hits = 4, untranslate_hits = 0
```

## Task 1.3

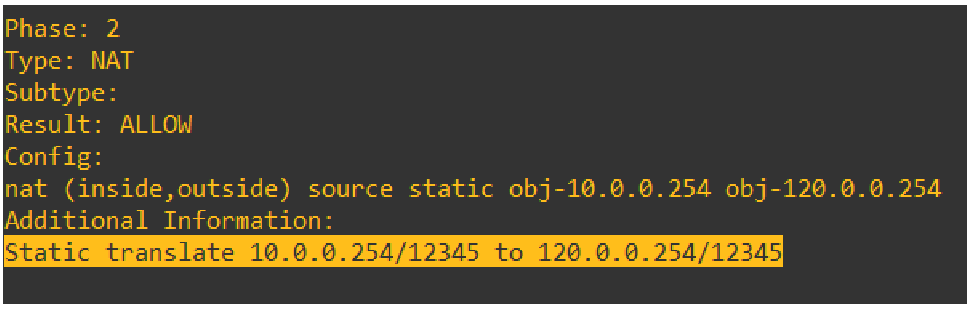
- **Configure Static NAT, Static Policy NAT, Static PAT and Twice NAT as per the following requirements:**

❖ Configure static bi-directional NAT on the ASA in such a way that host 10.0.0.254 and 172.16.1.3 (R3) get mapped to 120.0.0.254 and 120.0.0.3 respectively. Ensure that R2 synchronizes clock from the NTP server 10.0.0.254. You are allowed to create an ACL to achieve this requirement. Use Manual NAT to achieve this requirement.



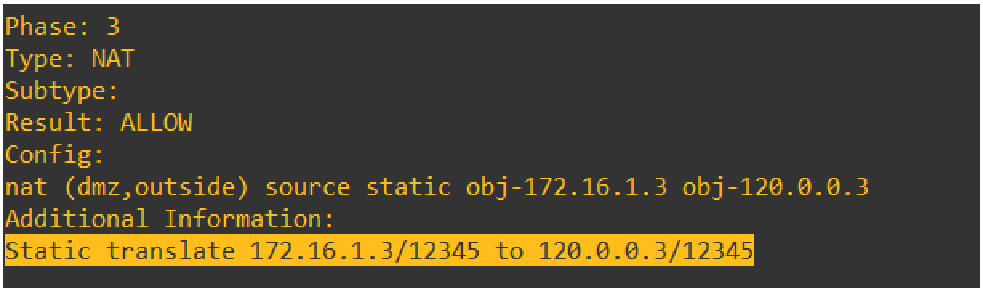
```
ASAv(config)# show run nat
nat (inside,outside) source static obj-10.0.0.254 obj-120.0.0.254
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.110-111 interface destinationm
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-grp-120.0.0.212-215 destination statim
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.130-131 interface destination3
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
nat (inside,outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
nat (dmz,outside) source static obj-172.16.1.3 obj-120.0.0.3
!
nat (inside,outside) after-auto source dynamic any interface
ASAv(config)#
```

### 10.0.0.254 get mapped to 120.0.0.254

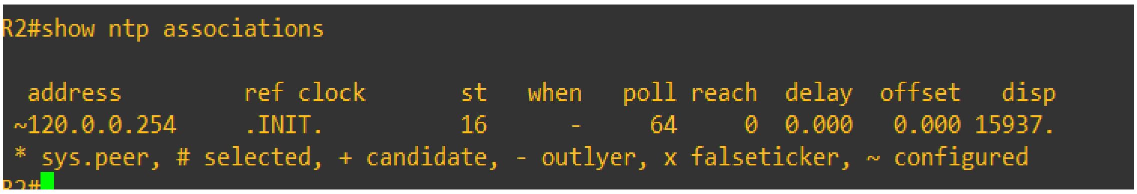


```
Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.0.254 obj-120.0.0.254
Additional Information:
Static translate 10.0.0.254/12345 to 120.0.0.254/12345
```

### 172.16.1.3 Get mapped to 120.0.0.3

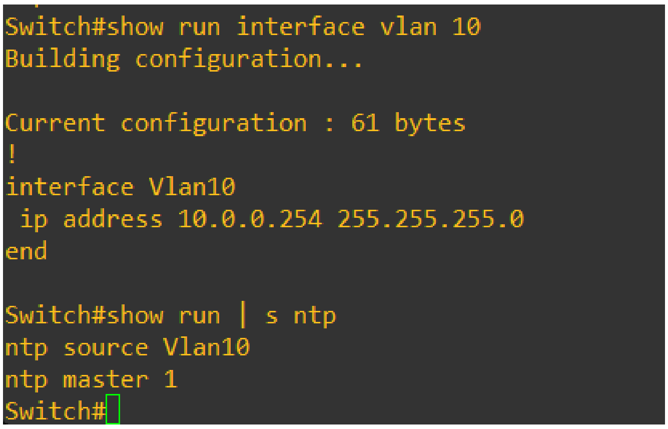


```
Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.1.3 obj-120.0.0.3
Additional Information:
Static translate 172.16.1.3/12345 to 120.0.0.3/12345
```



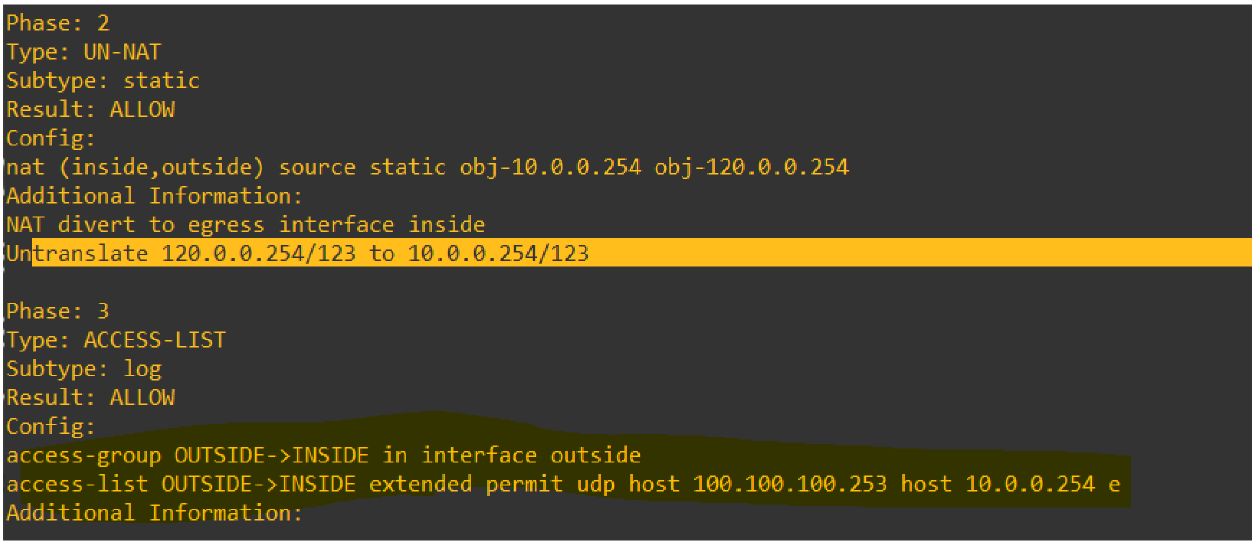
```
R2#show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
 ~120.0.0.254     .INIT.          16      -     64     0  0.000   0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R2#
```

### Switch Configuration



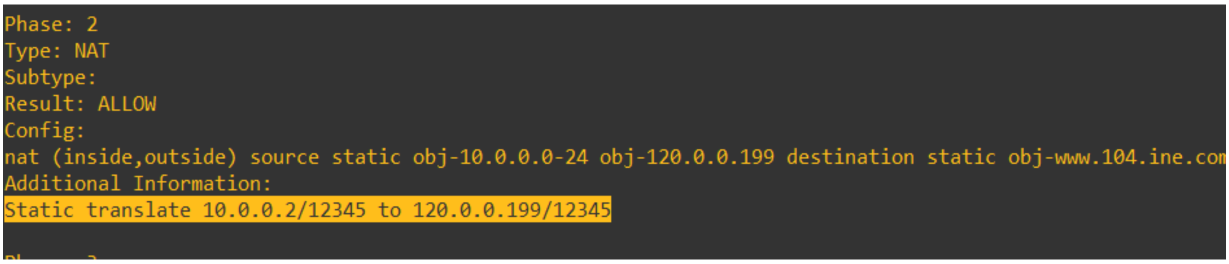
```
Switch#show run interface vlan 10
Building configuration...

Current configuration : 61 bytes
!
interface Vlan10
 ip address 10.0.0.254 255.255.255.0
end

Switch#show run | s ntp
ntp source Vlan10
ntp master 1
Switch#
```

**Running ACL:**



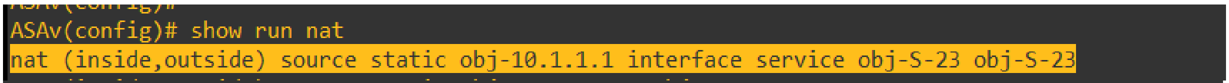
```
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.0.254 obj-120.0.0.254
Additional Information:
NAT divert to egress interface inside
Untranslate 120.0.0.254/123 to 10.0.0.254/123

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group OUTSIDE->INSIDE in interface outside
access-list OUTSIDE->INSIDE extended permit udp host 100.100.100.253 host 10.0.0.254 e
Additional Information:
```

- ❖ Configure static NAT on the ASA in such a way that if the subnet 10.0.0.0/24 does TELNET to www.104.ine.com, it gets translated using outside IP address 120.0.0.199.

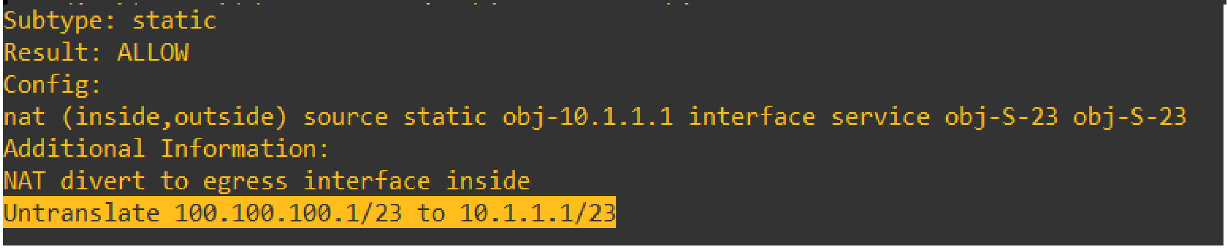


```
Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.0.0-24 obj-120.0.0.199 destination static obj-www.104.ine.com
Additional Information:
Static translate 10.0.0.2/12345 to 120.0.0.199/12345
```

- ❖ Configure static NAT on the ASA in such a way that TELNET sessions to the outside interface are redirected to R1's Loopback 0 interface. Use Manual NAT to achieve this.

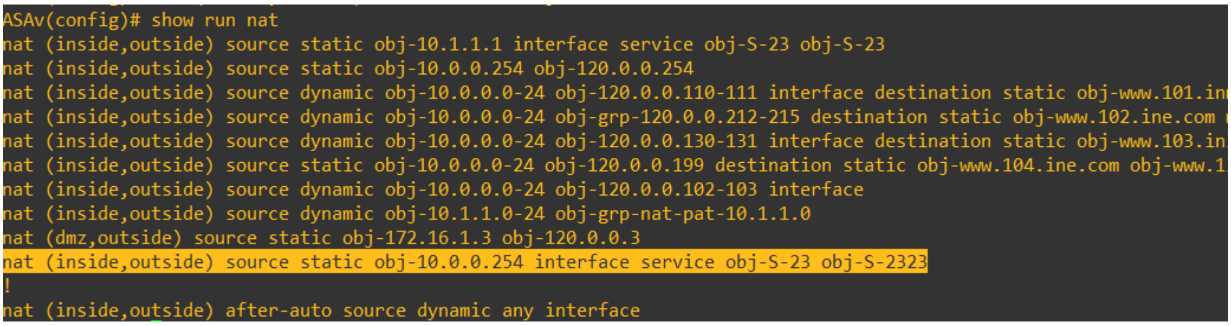


```
ASAv(config)# show run nat
nat (inside,outside) source static obj-10.1.1.1 interface service obj-S-23 obj-S-23
```



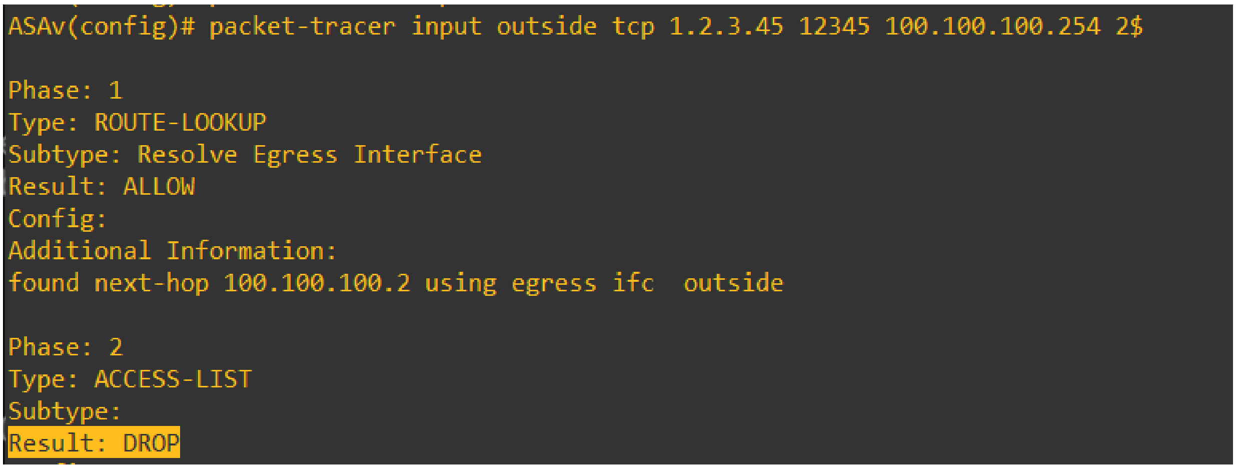
```
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.1.1.1 interface service obj-S-23 obj-S-23
Additional Information:
NAT divert to egress interface inside
Untranslate 100.100.100.1/23 to 10.1.1.1/23
```

- ❖ Configure the ASA in such a way that TELNET sessions to the outside interface on port 2323, are redirected to 10.0.0.254. Use Manual NAT to achieve this.



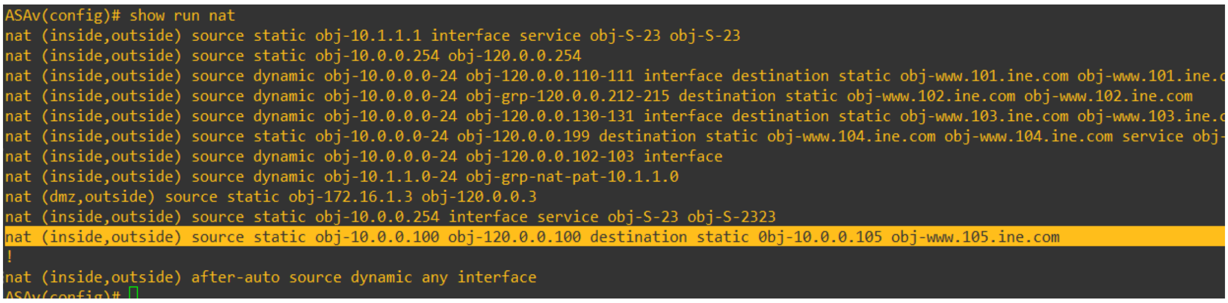
```
ASAv(config)# show run nat
nat (inside,outside) source static obj-10.1.1.1 interface service obj-S-23 obj-S-23
nat (inside,outside) source static obj-10.0.0.254 obj-120.0.0.254
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.110-111 interface destination static obj-www.101.in
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-grp-120.0.0.212-215 destination static obj-www.102.ine.com
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.130-131 interface destination static obj-www.103.in
nat (inside,outside) source static obj-10.0.0.0-24 obj-120.0.0.199 destination static obj-www.104.ine.com obj-www.1
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
nat (inside,outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
nat (dmz,outside) source static obj-172.16.1.3 obj-120.0.0.3
nat (inside,outside) source static obj-10.0.0.254 interface service obj-S-23 obj-S-2323
!
nat (inside,outside) after-auto source dynamic any interface
```

**Drop by ACL, because it does not match Access-List.**



```
ASAv(config)# packet-tracer input outside tcp 1.2.3.45 12345 100.100.100.254 2$

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 100.100.100.2 using egress ifc  outside

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
```

- ❖ Ensure 10.0.0.100 is statically translated to 120.0.0.100 and www.105.ine.com is statically translated to 10.0.0.105. Ensure both, Tony Stark and www.105.ine.com can access each other using their translated address.



```
ASAv(config)# show run nat
nat (inside,outside) source static obj-10.1.1.1 interface service obj-S-23 obj-S-23
nat (inside,outside) source static obj-10.0.0.254 obj-120.0.0.254
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.110-111 interface destination static obj-www.101.ine.com obj-www.101.ine.c
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-grp-120.0.0.212-215 destination static obj-www.102.ine.com obj-www.102.ine.com
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.130-131 interface destination static obj-www.103.ine.com obj-www.103.ine.c
nat (inside,outside) source static obj-10.0.0.0-24 obj-120.0.0.199 destination static obj-www.104.ine.com obj-www.104.ine.com service obj-
nat (inside,outside) source dynamic obj-10.0.0.0-24 obj-120.0.0.102-103 interface
nat (inside,outside) source dynamic obj-10.1.1.0-24 obj-grp-nat-pat-10.1.1.0
nat (dmz,outside) source static obj-172.16.1.3 obj-120.0.0.3
nat (inside,outside) source static obj-10.0.0.254 interface service obj-S-23 obj-S-2323
nat (inside,outside) source static obj-10.0.0.100 obj-120.0.0.100 destination static 0bj-10.0.0.105 obj-www.105.ine.com
!
nat (inside,outside) after-auto source dynamic any interface
ASAv(config)#
```

## NAT Concepts in ASA

1. **Dynamic NAT**

- Translates private IPs to a pool of public IPs.
- One-to-one mapping created dynamically when traffic flows.
- Requires at least as many public IPs as concurrent users.
- Used when multiple inside users need direct mapping to multiple public addresses.

2. **PAT (Port Address Translation)**

- Many private IPs share a single public IP.
- Differentiation happens using **port numbers**.
- Most common for internet access from private networks.
- Efficient because it conserves public IPv4 addresses.

3. **Dynamic Policy NAT / PAT**

- NAT decision is based on **source and destination** information.
- Allows different translation rules depending on where traffic is going.
- Example use: Same inside subnet may use PAT for Internet but a NAT pool for a partner network.

4. **Static NAT**

- Permanent one-to-one mapping between an internal IP and a public IP.
- Bidirectional: Both inside and outside can initiate traffic.
- Common for servers that must be reachable from the Internet (e.g., web, DNS).

5. **Static Policy NAT**

- Similar to static NAT, but translation depends on the **destination**.
- Allows one host to appear as different public IPs when accessing different external destinations.
- Useful in multi-ISP or business-to-business connections.

6. **Static PAT (Port Address Translation / Port Forwarding)**

- Maps one public IP to multiple internal hosts or services, using **port numbers**.
- Enables hosting multiple services (like web and SSH) on the same public IP.
- Often used when limited public IPs are available.

### 7. **Twice NAT (Manual NAT)**

- Translates both **source and destination** simultaneously.
- Useful when overlapping IP subnets exist between organizations.
- Provides very granular control of NAT policies.
- Can handle complex scenarios that regular static/dynamic NAT cannot.

## Comparison Table:

| NAT Type | Source Translation | Destination Translation | Static/Dynamic | Ports Used |
|---|---|---|---|---|
| Dynamic NAT | Yes | No | Dynamic | No |
| PAT | Yes | No | Dynamic | Yes |
| Policy NAT / PAT | Yes | Sometimes | Dynamic | Yes/No |
| Static NAT | Yes | No | Static | No |
| Static Policy NAT | Yes | Yes (conditional) | Static | No |
| Static PAT | Yes | No | Static | Yes |
| Twice NAT | Yes | Yes | Static/Dynamic | Yes/No |