

## Cấu hình static nat với object từ phiên bản 8.3 trở lên

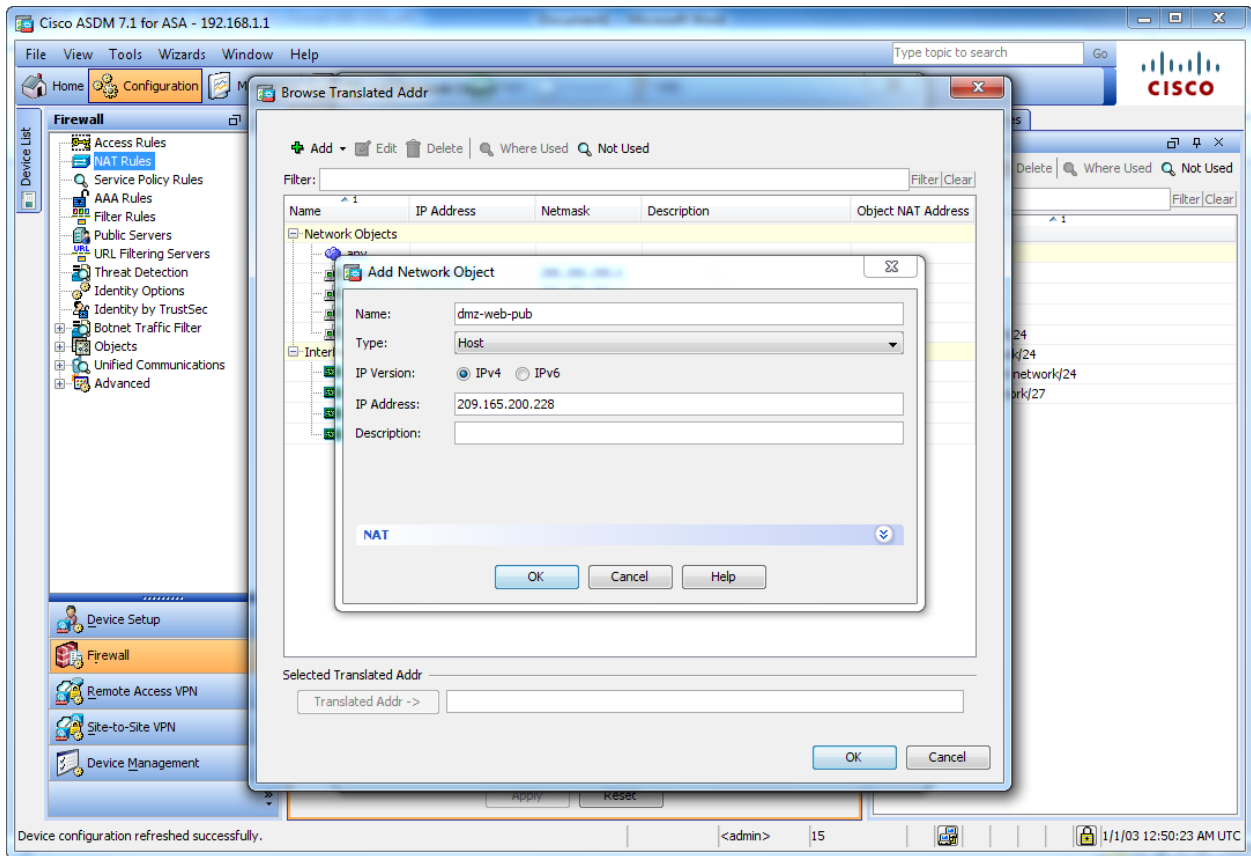
The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window shows the 'Firewall' configuration tree on the left, with 'NAT Rules' selected. The 'Add Network Object' dialog box is open, showing the following configuration:

- Name: dmz-web-priv
- Type: Host
- IP Version: IPv4 (selected)
- IP Address: 172.16.0.5
- Description: (empty)

The 'NAT' section is expanded, showing the following options:

- Add Automatic Address Translation Rules
- Type: Static
- Translated Addr: (empty)
- Use one-to-one address translation
- PAT Pool Translated Address: (empty)
- Round Robin
- Extend PAT uniqueness to per destination instead of per interface
- Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023
- Fall through to interface PAT(dest intf): dmz
- Use IPv6 for interface PAT

The 'Advanced...' button is visible below the NAT options. The 'OK', 'Cancel', and 'Help' buttons are at the bottom of the dialog box. The background shows the 'Network Objects' list with entries like 'any', 'any4', 'any6', 'dmz-network/24', 'inside-network/24', 'management-network/24', and 'outside-network/27'. The status bar at the bottom indicates 'Device configuration refreshed successfully.' and the user is logged in as '<admin>'.



Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Device configuration refreshed successfully.

<admin> 15 1/1/03 12:51:03 AM UTC

Browse Translated Addr

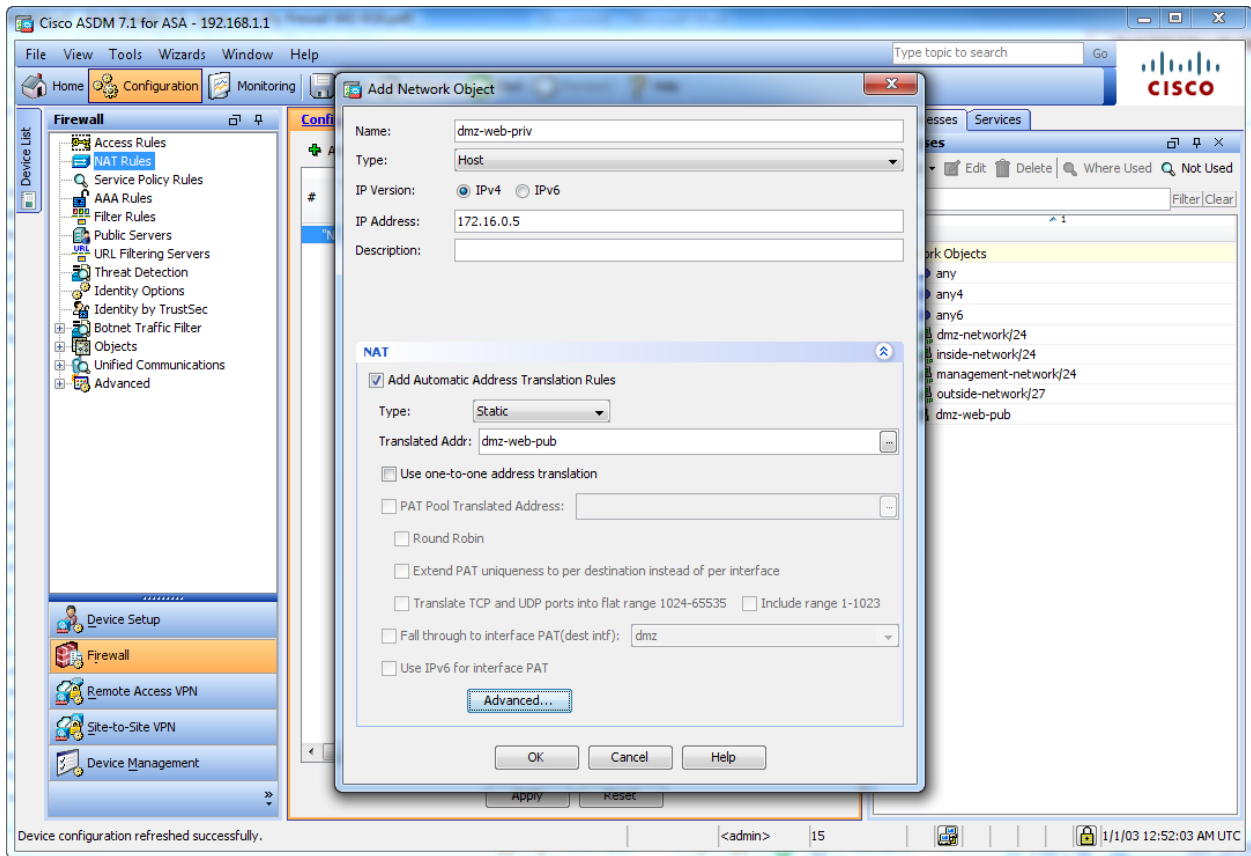
Filter: Filter Clear

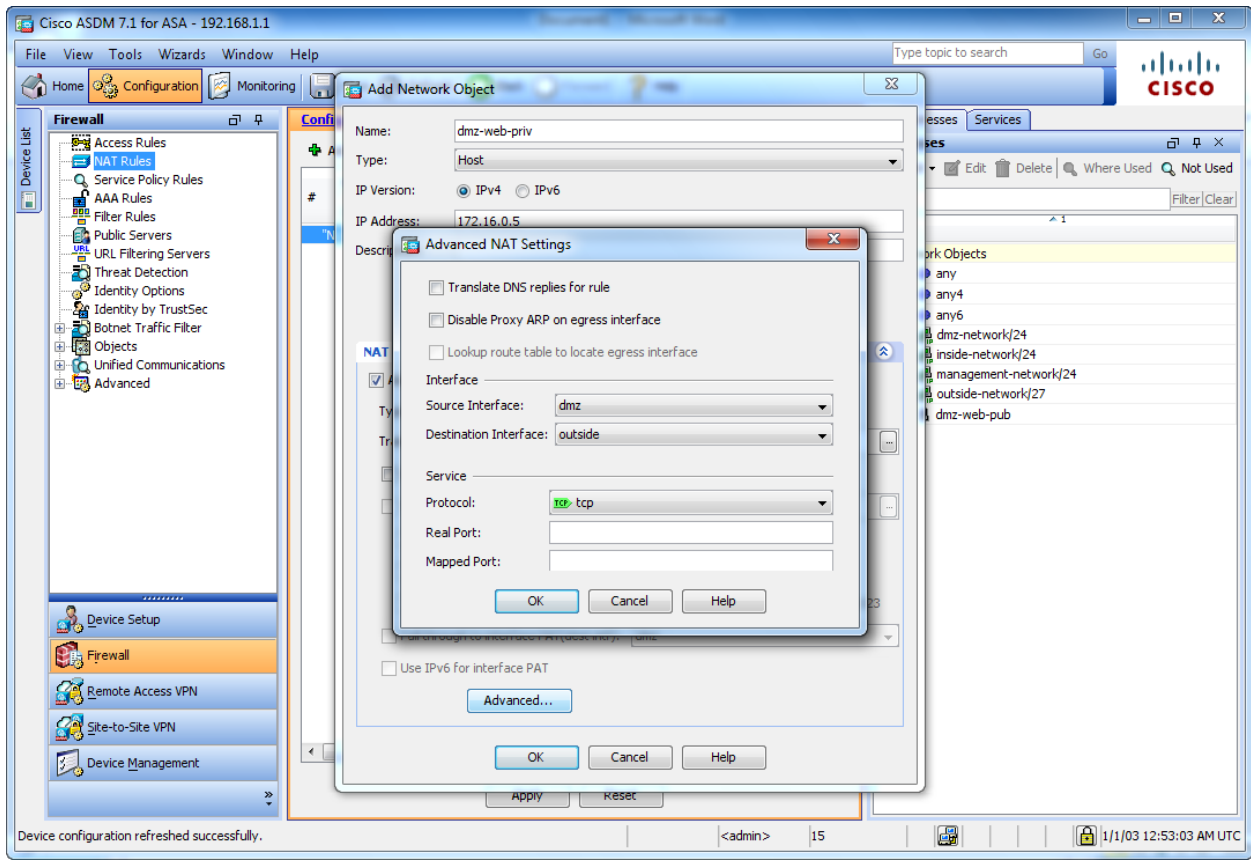
Name	IP Address	Netmask	Description	Object NAT Ad...
Network Objects				
any				
dmz-network	172.16.0.0	255.255.255.0		
inside-network	10.0.0.0	255.255.255.0		
management-network	192.168.1.0	255.255.255.0		
outside-network	209.165.200.224	255.255.255.224		
dmz-web-pub	209.165.200.228			
Interfaces				
dmz				
inside				
management				
outside				

Selected Translated Addr

Translated Addr -> |

OK Cancel





Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration > Firewall > NAT Rules

Add Edit Delete Find Diagram Packet Trace

#	Match Criteria: Original Packet					Action: Translated Packet			Opt
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	
"Network Object" NAT (Rule 1)									
1	dmz	outside	dmz-web-priv	any	any	dmz-web-pub...	-- Original --	-- Original --	
	outside	dmz	any	dmz-web-pub	any	-- Original -- (S)	dmz-web-priv	-- Original --	

Apply Reset

Configuration changes saved successfully.

<admin> 15 1/1/03 12:56:13 AM UTC

```
ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# object network dmz-web-pub
ciscoasa(config-network-object)# host 209.165.200.228
ciscoasa(config-network-object)# object network dmz-web-priv
ciscoasa(config-network-object)# host 172.16.0.5
ciscoasa(config-network-object)# nat (dmz,outside) static dmz-web-pub
ciscoasa(config-network-object)# _
Connected 0:00:39 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

## Cấu hình static pat

The screenshot displays the Cisco ASDM 7.1 for ASA - 192.168.1.1 interface. The main window shows the configuration of a static PAT rule named "dmz-https-priv". The rule is configured with the following parameters:

- Name: dmz-https-priv
- Type: Host
- IP Version: IPv4 (selected)
- IP Address: 172.16.0.15

The "Advanced NAT Settings" dialog box is open, showing the following configuration:

- Translate DNS replies for rule
- Disable Proxy ARP on egress interface
- Lookup route table to locate egress interface
- Interface
- Source Interface: dmz
- Destination Interface: outside
- Service
- Protocol: tcp
- Real Port: 8443
- Mapped Port: 443

The "Advanced NAT Settings" dialog box also includes an "Advanced..." button and "OK", "Cancel", and "Help" buttons. The main configuration window includes "Apply" and "Reset" buttons.

The status bar at the bottom of the window shows "Device configuration refreshed successfully." and the user is logged in as "admin" with the IP address "15". The system time is "1/1/03 1:13:23 AM UTC".



Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Add Network Object

Device List

- Firewall
  - Access Rules
  - NAT Rules
  - Service Policy Rules
  - AAA Rules
  - Filter Rules
  - Public Servers
  - URL Filtering Servers
  - Threat Detection
  - Identity Options
  - Identity by TrustSec
  - Botnet Traffic Filter
  - Objects
  - Unified Communications
  - Advanced
- Device Setup
- Firewall
- Remote Access VPN
- Site-to-Site VPN
- Device Management

Configuration

Name: dmz-https-priv  
Type: Host  
IP Version: IPv4 IPv6  
IP Address: 172.16.0.15  
Description:

NAT

Add Automatic Address Translation Rules

Type: Static

Translated Addr: dmz-pat-outside

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

Fall through to interface PAT(dest intf): dmz

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

Related Packet

Destination	Service	Opt
dmz-https-priv	https	Original
dmz-web-priv	web	Original

Apply Reset

Device configuration refreshed successfully.

<admin> 15 1/1/03 1:13:23 AM UTC

Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

CISCO

**Firewall**

- Access Rules
- NAT Rules**
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Device Setup  
**Firewall**  
 Remote Access VPN  
 Site-to-Site VPN  
 Device Management

**Configuration > Firewall > NAT Rules**

#	Match Criteria: Original Packet			Action: Translated Packet			Opt	
	Source Intf	Dest Intf	Source	Destination	Service	Source		Destination
<b>*Network Object* NAT (Rule 1)</b>								
1	dmz	outside	dmz-web-priv	any	any	dmz-web-pub...	-- Original --	-- Original --
	outside	dmz	any	dmz-web-pub	any	-- Original -- (S)	dmz-web-priv	-- Original --
2	dmz	outside	dmz-https-priv	any	8443	dmz-pat-outsi...	-- Original --	https
	outside	dmz	any	dmz-pat-out...	https	-- Original -- (S)	dmz-https-priv	8443

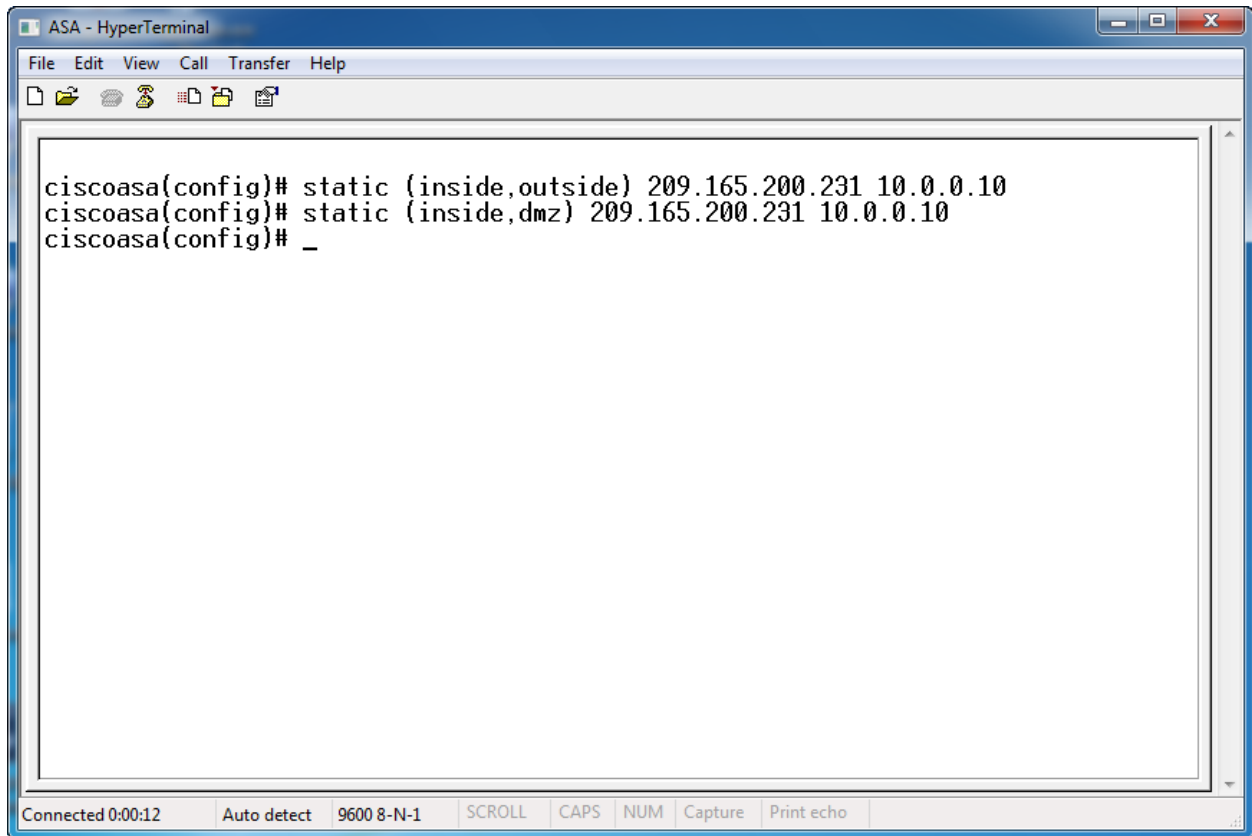
Apply Reset

Configuration changes saved successfully.

<admin> 15 1/1/03 1:18:41 AM UTC

```
ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# object network dmz-pat-outside
ciscoasa(config-network-object)# host 209.165.200.230
ciscoasa(config-network-object)# object network dmz-https-priv
ciscoasa(config-network-object)# host 172.16.0.15
ciscoasa(config-network-object)# nat (dmz,outside) static dmz-pat-outside serv$
ciscoasa(config-network-object)# _
Connected 0:00:32 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

## Cấu hình static trên IOS 8.2 trở xuống

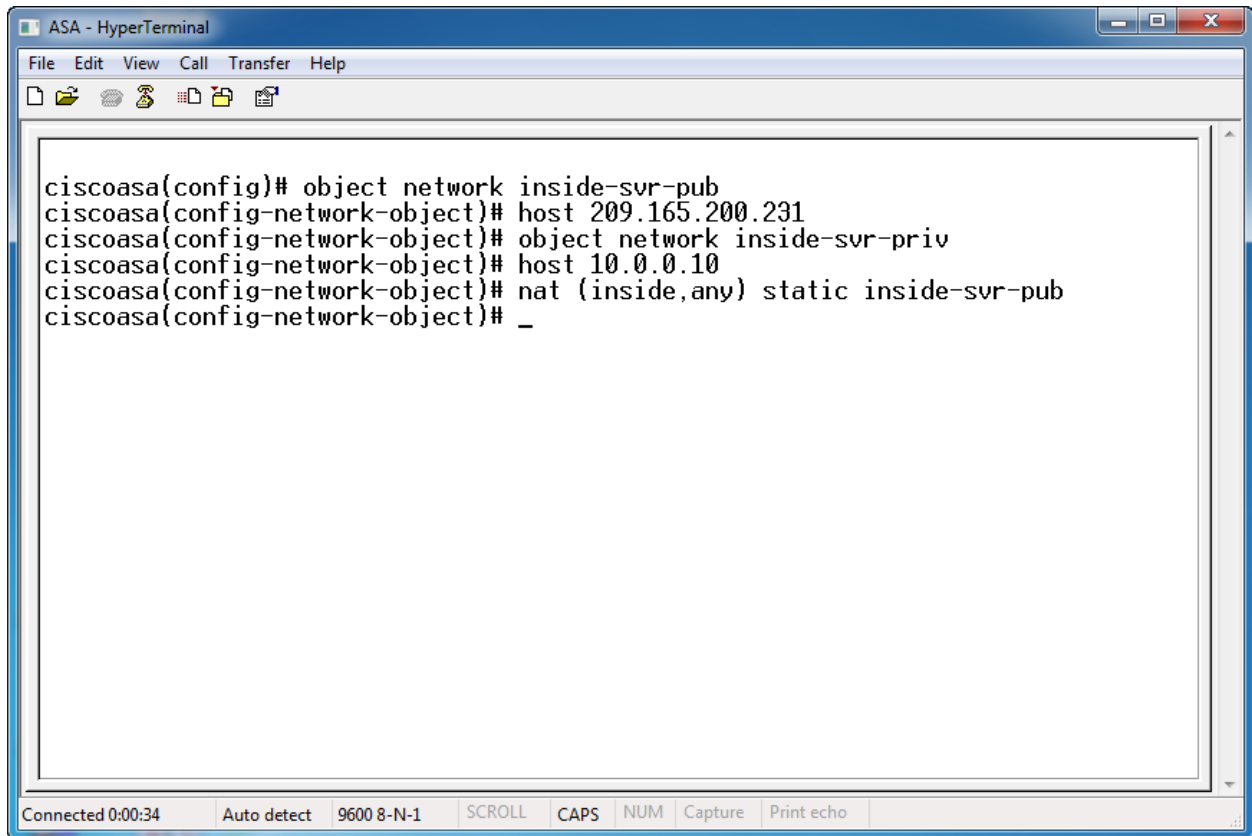


The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a terminal session with the following text:

```
ciscoasa(config)# static (inside,outside) 209.165.200.231 10.0.0.10
ciscoasa(config)# static (inside,dmz) 209.165.200.231 10.0.0.10
ciscoasa(config)# _
```

The bottom status bar of the window displays: "Connected 0:00:12", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

## Cấu hình static với IOS 8.3 trở lên



```
ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# object network inside-svr-pub
ciscoasa(config-network-object)# host 209.165.200.231
ciscoasa(config-network-object)# object network inside-svr-priv
ciscoasa(config-network-object)# host 10.0.0.10
ciscoasa(config-network-object)# nat (inside,any) static inside-svr-pub
ciscoasa(config-network-object)# _
Connected 0:00:34 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

## Cấu hình dynamic NAT

The screenshot displays the Cisco ASDM 7.1 for ASA - 192.168.1.1 interface. The main window shows the configuration of a network object named "inside-seg". The configuration is as follows:

- Name: inside-seg
- Type: Network
- IP Version: IPv4 (selected)
- IP Address: 10.0.0.0
- Netmask: 255.255.255.0
- Description: (empty)

The NAT configuration section is expanded, showing the following options:

- Add Automatic Address Translation Rules
- Type: Dynamic
- Translated Addr: (empty)
- Use one-to-one address translation
- PAT Pool Translated Address: (empty)
- Round Robin
- Extend PAT uniqueness to per destination instead of per interface
- Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023
- Fall through to interface PAT(dest intf): dmz
- Use IPv6 for interface PAT

The "Advanced..." button is visible below the NAT options. The bottom status bar shows "Configuration changes saved successfully." and the user is logged in as "admin" with a session ID of "15". The system time is "1/1/03 1:42:31 AM UTC".

Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration changes saved successfully.

<admin> 15 1/1/03 1:42:31 AM UTC

**Browse Translated Addr**

Filter: [ ] Filter Clear

Name	IP Address	Netmask	Description	Object NAT Ad...
Network Objects				
dmz-http-obj	172.16.0.15			
Add Network Object				
Name:	outside-nat-pool			
Type:	Range			
IP Version:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6			
Start Address:	209.165.200.235			
End Address:	209.165.200.254			
Description:				
NAT				

Selected Translated Addr

Translated Addr -> [ ]

OK Cancel Help

OK Cancel

Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration

Firewall

- Access Rules
- NAT Rules**
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration changes saved successfully.

<admin> 15 1/1/03 1:42:31 AM UTC

### Browse Translated Addr

Filter:  Filter Clear

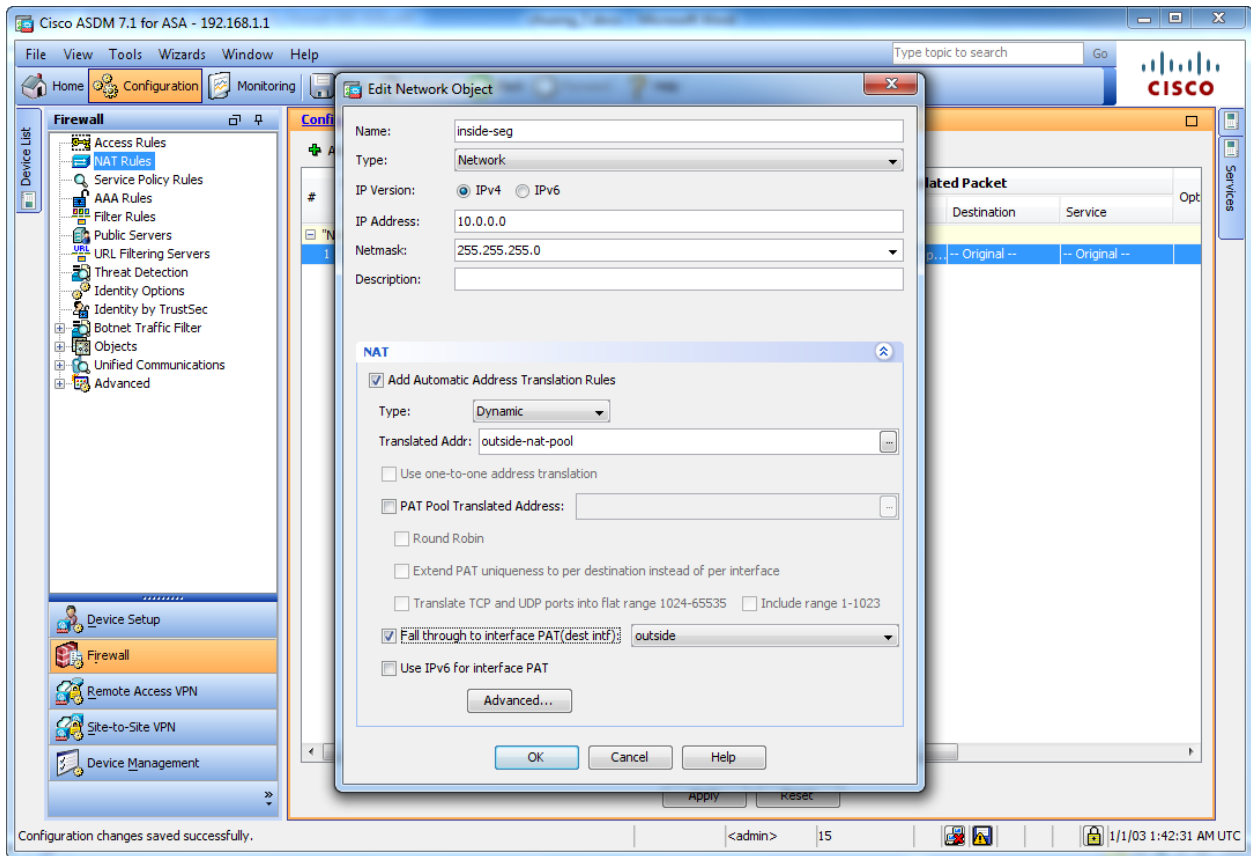
Name	IP Address	Netmask	Description	Object NAT Ad...
Network Objects				
dmz-https-priv	172.16.0.15			
dmz-pat-outside	209.165.200.230			
dmz-web-priv	172.16.0.5			
dmz-web-pub	209.165.200.228			
inside-svr-priv	10.0.0.10			
inside-svr-pub	209.165.200.231			
outside-nat-pool	209.165.200.235-2...			
Interfaces				
dmz				
inside				
management				
outside				

Selected Translated Addr

Translated Addr ->

OK Cancel





Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Configuration > Firewall > NAT Rules

Device List

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Match Criteria: Original Packet

Action: Translated Packet

#	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	Opt
"Network Object" NAT (Rule 1)									
1	Any	outside	inside-seg	any	any	outside-nat-p...	outside	-- Original --	

Apply Reset

Configuration changes saved successfully.

<admin> 15 1/1/03 1:42:31 AM UTC

## Cấu hình dynamic PAT (HIDE)

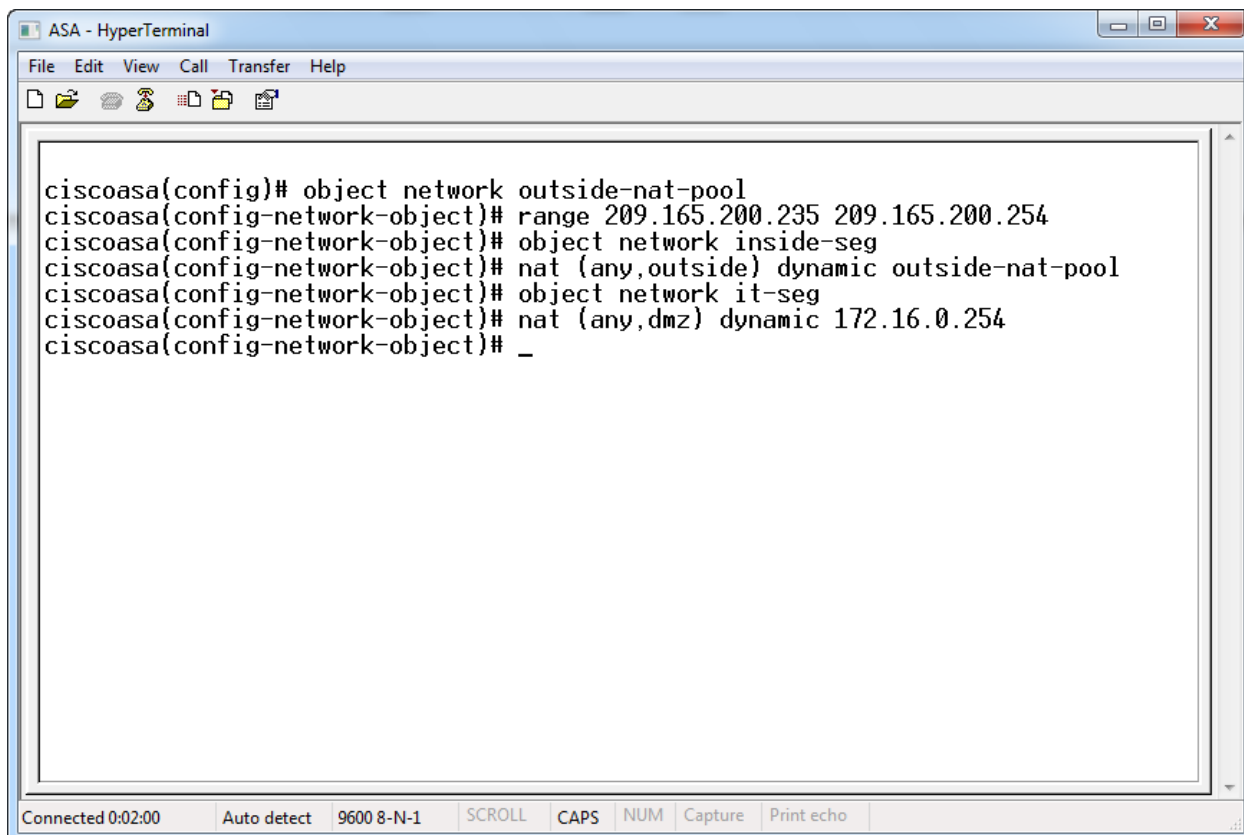
The screenshot shows the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Cisco ASDM 7.1 for ASA - 192.168.1.1". The left sidebar shows the "Firewall" configuration tree, with "NAT Rules" selected. The main content area displays the "Add Network Object" dialog box, which is used to configure a new network object. The dialog box has the following fields and options:

- Name: it-seg
- Type: Network
- IP Version: IPv4 (selected), IPv6
- IP Address: 10.0.1.0
- Netmask: 255.255.255.0
- Description:

The "NAT" section is expanded, showing the following options:

- Add Automatic Address Translation Rules
- Type: Dynamic PAT (Hide)
- Translated Addr: 172.16.0.254
- Use one-to-one address translation
- PAT Pool Translated Address:
- Round Robin
- Extend PAT uniqueness to per destination instead of per interface
- Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023
- Fall through to interface PAT(dest intf): dmz
- Use IPv6 for interface PAT

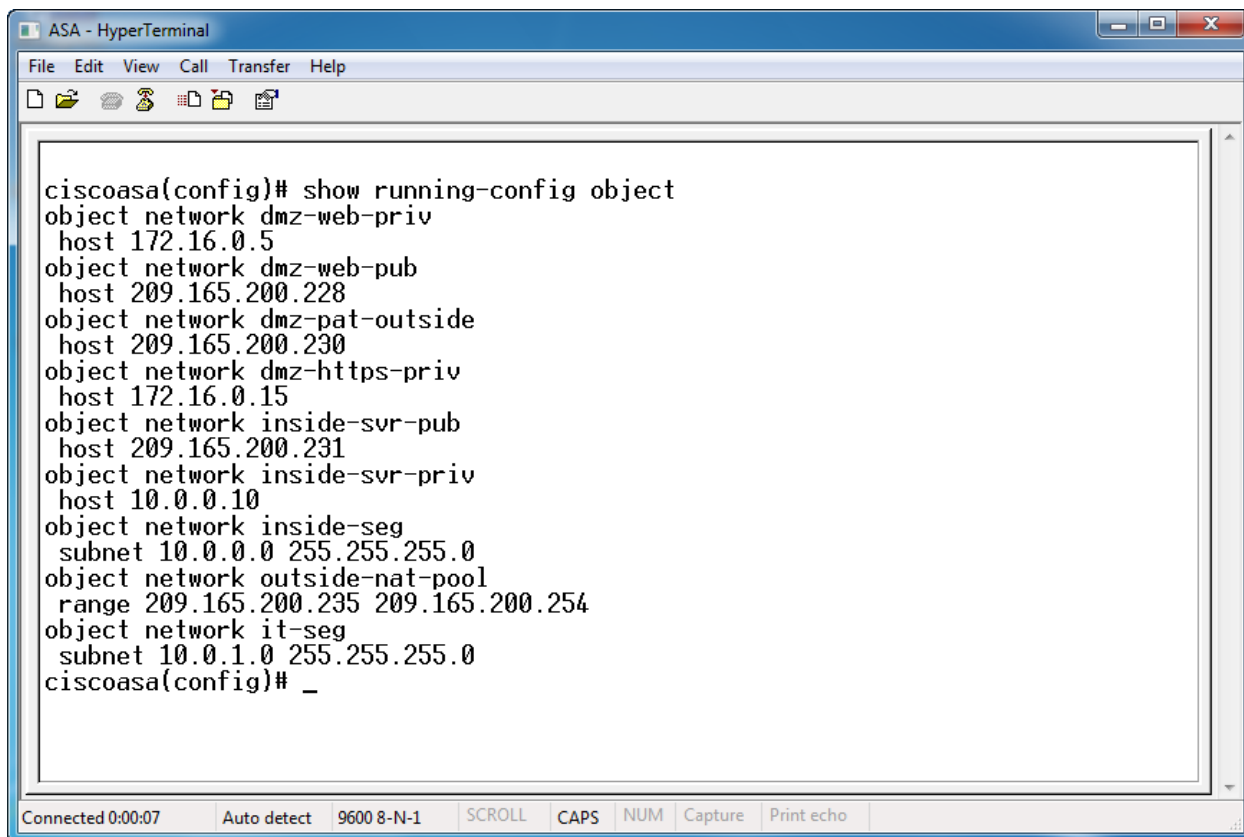
The dialog box has "OK", "Cancel", and "Help" buttons. The "Advanced..." button is also visible. The status bar at the bottom shows "Configuration changes saved successfully." and the user is logged in as "admin" with a session ID of "15". The system time is "1/1/03 1:42:31 AM UTC".



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a series of configuration commands for a Cisco ASA device. The commands are as follows:

```
ciscoasa(config)# object network outside-nat-pool
ciscoasa(config-network-object)# range 209.165.200.235 209.165.200.254
ciscoasa(config-network-object)# object network inside-seg
ciscoasa(config-network-object)# nat (any,outside) dynamic outside-nat-pool
ciscoasa(config-network-object)# object network it-seg
ciscoasa(config-network-object)# nat (any,dmz) dynamic 172.16.0.254
ciscoasa(config-network-object)# _
```

The bottom status bar of the HyperTerminal window displays the following information: "Connected 0:02:00", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".



```
ciscoasa(config)# show running-config object
object network dmz-web-priv
  host 172.16.0.5
object network dmz-web-pub
  host 209.165.200.228
object network dmz-pat-outside
  host 209.165.200.230
object network dmz-https-priv
  host 172.16.0.15
object network inside-svr-pub
  host 209.165.200.231
object network inside-svr-priv
  host 10.0.0.10
object network inside-seg
  subnet 10.0.0.0 255.255.255.0
object network outside-nat-pool
  range 209.165.200.235 209.165.200.254
object network it-seg
  subnet 10.0.1.0 255.255.255.0
ciscoasa(config)# _
```

Connected 0:00:07    Auto detect    9600 8-N-1    SCROLL    CAPS    NUM    Capture    Print echo