

Cấu hình NAT CONTROL

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Firewall > NAT Rules". The interface includes a menu bar (File, View, Tools, Wizards, Window, Help), a toolbar with icons for Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help, and a search bar. On the left, a "Device List" pane shows a tree view of configuration objects: Access Rules, NAT Rules (selected), Service Policy Rules, AAA Rules, Filter Rules, Public Servers, URL Filtering Servers, Threat Detection, Botnet Traffic Filter, Objects, Unified Communications, and Advanced. Below this is a "Device Setup" pane with buttons for Device Setup, Firewall (selected), Remote Access VPN, Site-to-Site VPN, and Device Management. The main configuration area contains a table for NAT Rules with columns: #, Type, Original (Source, Destination), and Translated (Service, Interface). The table is currently empty. Below the table is a checkbox labeled "Enable traffic through the firewall without address translation" which is unchecked. At the bottom of the main area are "Apply" and "Reset" buttons. On the right, a "Addresses" pane is open, showing a list of network objects: IPv4 Network Objects (any, management-network/24) and IPv6 Network Objects (any). The status bar at the bottom indicates "Configuration changes saved successfully.", the user is "<admin>", and the page number is "15". The system clock shows "4/4/14 8:22:29 AM UTC".

```
ASA - HyperTerminal
File Edit View Call Transfer Help
[Icons]
ciscoasa(config)# nat-control
ciscoasa(config)# _
Connected 0:00:51 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Cấu hình Dynamic Inside NAT

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Firewall > NAT Rules". A dialog box titled "Add Global Address Pool" is open, showing the configuration for a new address pool. The "Interface" is set to "outside" and the "Pool ID" is "1". Under "IP Addresses to Add", the "Range" option is selected, with the "Starting IP Address" set to "209.165.200.235", the "Ending IP Address" set to "209.165.200.254", and the "Netmask (optional)" set to "255.255.255.224". The "Addresses Pool" list on the right shows the added range: "209.165.200.235 - 209.165.200.254". The "Port Address Translation (PAT)" options are not selected. The "Enable traffic through the firewall without address translation" checkbox is also unchecked. The status bar at the bottom indicates "Device configuration refreshed successfully." and the user is logged in as "<admin>" with the session ID "15". The system time is "4/4/14 8:45:19 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

Firewall

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

Configuration > Firewall > NAT Rules

Addresses Services Global Pools

Addresses

Filter: Where Used

Filter: Clear

Network Objects

- any
- inside-network/24
- management-network/24
- Network Objects
- any

Device List

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

Add Dynamic NAT Rule

Original

Interface: inside

Source: inside-network/24

Translated

Select a global pool for dynamic translation.

| Pool ID | Interface | Addresses Pool |
|---------|------------|-------------------------------------|
| 0 | (outbound) | Same as original address (identity) |
| 0 | (inbound) | Same as original address (identity) |

Manage...

Connection Settings

OK Cancel Help

Enable traffic through the firewall without address translation

Apply Reset

Device configuration refreshed successfully.

<admin> 15

4/4/14 8:43:29 AM UTC

Cisco ASDM 7.1 for ASA - 192.168.1.1

Configuration > Firewall > NAT Rules

Original

| # | Type | Original | Translated |
|---|------|----------|------------|
| | | | |

Add Dynamic NAT Rule

Original

Interface: inside

Source: inside-network/24

Translated

Select a global pool for dynamic translation.

| Pool ID | Interface | Addresses Pool |
|---------|------------|-------------------------------------|
| 0 | (outbound) | Same as original address (identity) |
| 0 | (inbound) | Same as original address (identity) |
| 1 | outside | 209.165.200.235 - 209.165.200.254 |

Manage...

Connection Settings

OK Cancel Help

Apply Reset

Device configuration refreshed successfully.

<admin> 15 4/4/14 8:46:19 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

Firewall

- Access Rules
- NAT Rules**
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- 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

| # | Type | Original | | Translated | | |
|--------|---------|-------------------|-------------|------------|-----------|-----------------------------------|
| | | Source | Destination | Service | Interface | Address |
| inside | | | | | | |
| 1 | Dynamic | inside-network/24 | | | outside | 209.165.200.235 - 209.165.200.254 |

Enable traffic through the firewall without address translation

Apply Reset

<admin> 15 4/4/14 8:48:29 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

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced
 - Anti-Spoofing
 - Certificate Management
 - Fragment
 - IP Audit
 - SUNRPC Server
 - TCP Options
 - Global Timeouts
 - Virtual Access
 - ACL Manager
 - Standard ACL
 - Per-Session NAT Rules

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration > Firewall > Advanced > Global Timeouts

Specify the maximum idle time intervals using the hh:mm:ss format.

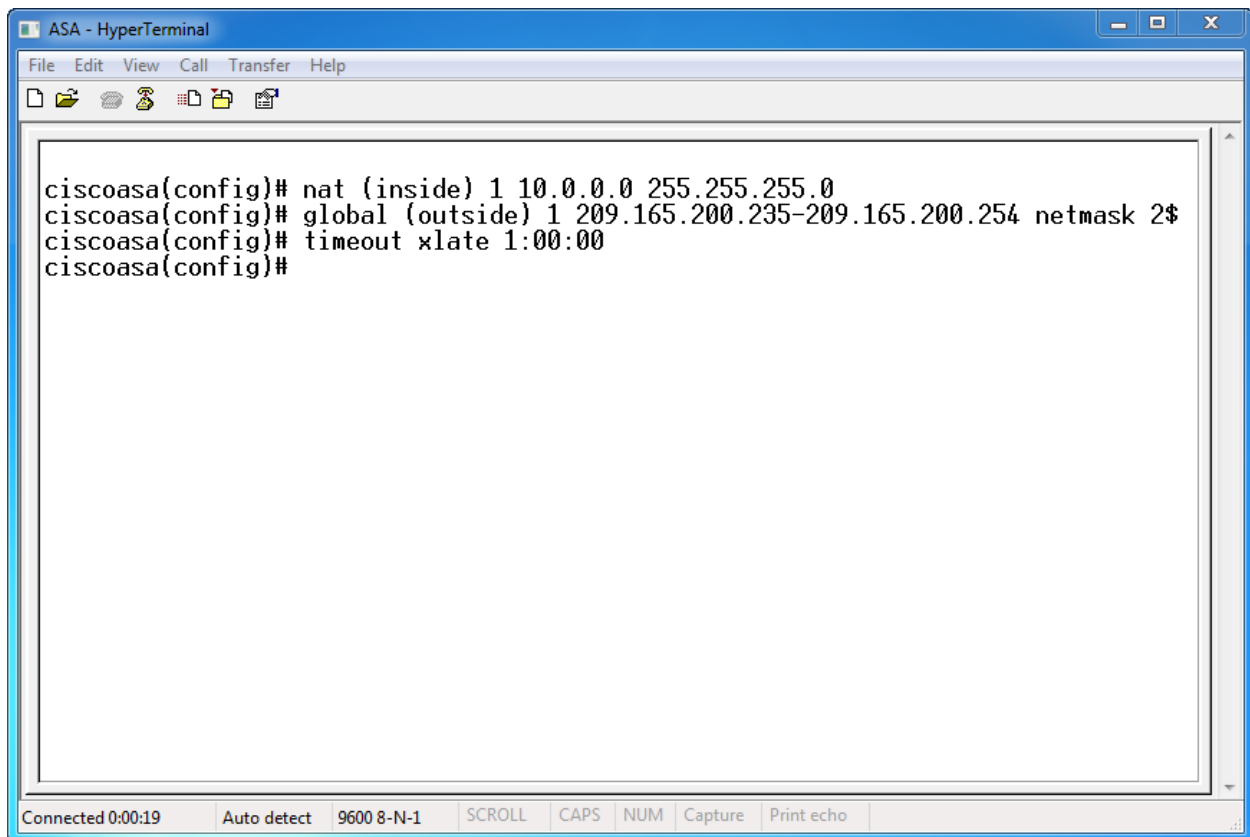
Disabling a timeout setting reverts it to the default value. If both absolute and inactivity authentication timeouts are set to 00:00:00, the user will have to re-authenticate on every new connection.

| | | | |
|---|----------|--|----------|
| <input type="checkbox"/> Connection | 01:00:00 | <input type="checkbox"/> SUNRPC | 00:10:00 |
| <input type="checkbox"/> Half-closed | 00:10:00 | <input type="checkbox"/> SIP | 00:30:00 |
| <input type="checkbox"/> UDP | 00:02:00 | <input type="checkbox"/> SIP Media | 00:02:00 |
| <input type="checkbox"/> ICMP | 00:00:02 | <input type="checkbox"/> SIP Provisional Media | 00:02:00 |
| <input type="checkbox"/> H.323 | 00:05:00 | <input type="checkbox"/> SIP Invite | 00:03:00 |
| <input type="checkbox"/> H.225 | 01:00:00 | <input type="checkbox"/> SIP Disconnect | 00:02:00 |
| <input type="checkbox"/> MGCP | 00:05:00 | <input type="checkbox"/> Authentication absolute | 00:05:00 |
| <input type="checkbox"/> MGCP PAT | 00:05:00 | <input type="checkbox"/> Authentication inactivity | 00:00:00 |
| <input type="checkbox"/> TCP Proxy Reassembly | 00:01:00 | <input checked="" type="checkbox"/> Translation Slot | 01:00:00 |

Apply Reset

Configuration changes saved successfully.

<admin> 15 4/4/14 8:49:29 AM UTC



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

```
ciscoasa(config)# nat (inside) 1 10.0.0.0 255.255.255.0
ciscoasa(config)# global (outside) 1 209.165.200.235-209.165.200.254 netmask 255.255.255.0
ciscoasa(config)# timeout xlate 1:00:00
ciscoasa(config)#
```

The status bar at the bottom of the window displays: "Connected 0:00:19", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

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
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced
 - Anti-Spoofing
 - Certificate Management
 - Fragment
 - IP Audit
 - SUNRPC Server
 - TCP Options
 - Global Timeouts
 - Virtual Access
 - ACL Manager
 - Standard ACL
 - Per-Session NAT Rules

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration > Firewall > NAT Rules

| # | Type | Original | Translated |
|---|------|----------|---------------------------|
| | | | 100.235 - 209.165.200.254 |

Add Global Address Pool

Interface: dmz

Pool ID: 5

IP Addresses to Add

- Range
 - Starting IP Address:
 - Ending IP Address:
 - Netmask (optional):
- Port Address Translation (PAT)
 - IP Address: 172.16.0.254
 - Netmask (optional): 255.255.255.255
- Port Address Translation (PAT) using IP Address of the interface

Addresses Pool

- 172.16.0.254

Buttons: Add >>, << Delete, OK, Cancel, Help

Enable traffic through the firewall without address translation

Apply Reset

Device configuration refreshed successfully.

<admin> 15 4/4/14 8:56:59 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

Firewall

Configuration > Firewall > NAT Rules

Original Translated

Type Original Translated

00.235 - 209.165.200.254

Global Pools

Device List

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced
 - Anti-Spoofing
 - Certificate Management
 - Fragment
 - IP Audit
 - SUNRPC Server
 - TCP Options
 - Global Timeouts
 - Virtual Access
 - ACL Manager
 - Standard ACL
 - Per-Session NAT Rules

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Device configuration refreshed successfully.

<admin> 15

4/4/14 8:58:59 AM UTC

Original

Interface: inside

Source: inside-network/24

Translated

Select a global pool for dynamic translation.

| Pool ID | Interface | Addresses Pool |
|---------|------------|-------------------------------------|
| 0 | (outbound) | Same as original address (identity) |
| 0 | (inbound) | Same as original address (identity) |
| 1 | outside | 209.165.200.235 - 209.165.200.254 |
| 5 | dmz | 172.16.0.254 |

Manage...

Connection Settings

OK Cancel Help

Enable traffic through the firewall without address translation

Apply Reset

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
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced
 - Anti-Spoofing
 - Certificate Management
 - Fragment
 - IP Audit
 - SUNRPC Server
 - TCP Options
 - Global Timeouts
 - Virtual Access
 - ACL Manager
 - Standard ACL
 - Per-Session NAT Rules

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Configuration > Firewall > NAT Rules

Add Edit Delete Find Diagram Packet Trace

| # | Type | Original | Translated |
|---|------|----------|--------------------------|
| | | | 00.235 - 209.165.200.254 |

Add Global Address Pool

Interface: outside

Pool ID: 5

IP Addresses to Add

- Range
 - Starting IP Address:
 - Ending IP Address:
 - Netmask (optional):
- Port Address Translation (PAT)
 - IP Address:
 - Netmask (optional):
- Port Address Translation (PAT) using IP Address of the interface

Addresses Pool

- asa/outside

Buttons: Add >>, << Delete, OK, Cancel, Help

Enable traffic through the firewall without address translation

Apply Reset

Device configuration refreshed successfully.

<admin> 15 4/4/14 8:58:09 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

Firewall

Configuration > Firewall > NAT Rules

Original Translated

Type Original Translated

00.235 - 209.165.200.254

Global Pools

Device List

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced
 - Anti-Spoofing
 - Certificate Management
 - Fragment
 - IP Audit
 - SUNRPC Server
 - TCP Options
 - Global Timeouts
 - Virtual Access
 - ACL Manager
 - Standard ACL
 - Per-Session NAT Rules

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Device configuration refreshed successfully.

<admin> 15 4/4/14 8:59:39 AM UTC

Original

Interface: inside

Source: inside-network/24

Translated

Select a global pool for dynamic translation.

| Pool ID | Interface | Addresses Pool |
|---------|------------|-------------------------------------|
| 0 | (outbound) | Same as original address (identity) |
| 0 | (inbound) | Same as original address (identity) |
| 1 | outside | 209.165.200.235 - 209.165.200.254 |
| 5 | dmz | 172.16.0.254 |
| | outside | outside |

Manage...

Connection Settings

OK Cancel Help

Apply Reset

Enable traffic through the firewall without address translation

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
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced
 - Anti-Spoofing
 - Certificate Management
 - Fragment
 - IP Audit
 - SUNRPC Server
 - TCP Options
 - Global Timeouts
 - Virtual Access
 - ACL Manager
 - Standard ACL
 - Per-Session NAT Rules

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

Configuration > Firewall > NAT Rules

+ Add - Edit Delete | Find Diagram Packet Trace

| # | Type | Original | | Translated | | |
|--------|---------|-------------------|-------------|------------|-----------|--------------|
| | | Source | Destination | Service | Interface | Address |
| inside | | | | | | |
| 1 | Dynamic | inside-network/24 | | | dmz | 172.16.0.254 |
| 2 | | | | | outside | outside |

Enable traffic through the firewall without address translation

Apply Reset

Configuration changes saved successfully.

<admin> 15 4/4/14 9:00:49 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

Firewall

Configuration > Firewall > NAT Rules

Add Edit Delete Find Diagram Packet Trace

Original Translated

Type Original Translated

254

global Pools

Device List

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced
 - Anti-Spoofing
 - Certificate Management
 - Fragment
 - IP Audit
 - SUNRPC Server
 - TCP Options
 - Global Timeouts
 - Virtual Access
 - ACL Manager
 - Standard ACL
 - Per-Session NAT Rules

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

Add Dynamic NAT Rule

Original

Interface: dmz

Source: dmz-network/24

Translated

Select a global pool for dynamic translation.

| Pool ID | Interface | Addresses Pool |
|---------|------------|-------------------------------------|
| 0 | (outbound) | Same as original address (identity) |
| 0 | (inbound) | Same as original address (identity) |
| 1 | outside | 209.165.200.235 - 209.165.200.254 |
| 5 | outside | dmz outside |

Manage...

Connection Settings

OK Cancel Help

Enable traffic through the firewall without address translation

Apply Reset

Device configuration refreshed successfully.

<admin> 15 4/4/14 9:04:39 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

Firewall

- Access Rules
- NAT Rules**
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced
 - Anti-Spoofing
 - Certificate Management
 - Fragment
 - IP Audit
 - SUNRPC Server
 - TCP Options
 - Global Timeouts
 - Virtual Access
 - ACL Manager
 - Standard ACL
 - Per-Session NAT Rules

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

Configuration > Firewall > NAT Rules

Add Edit Delete Find Diagram Packet Trace

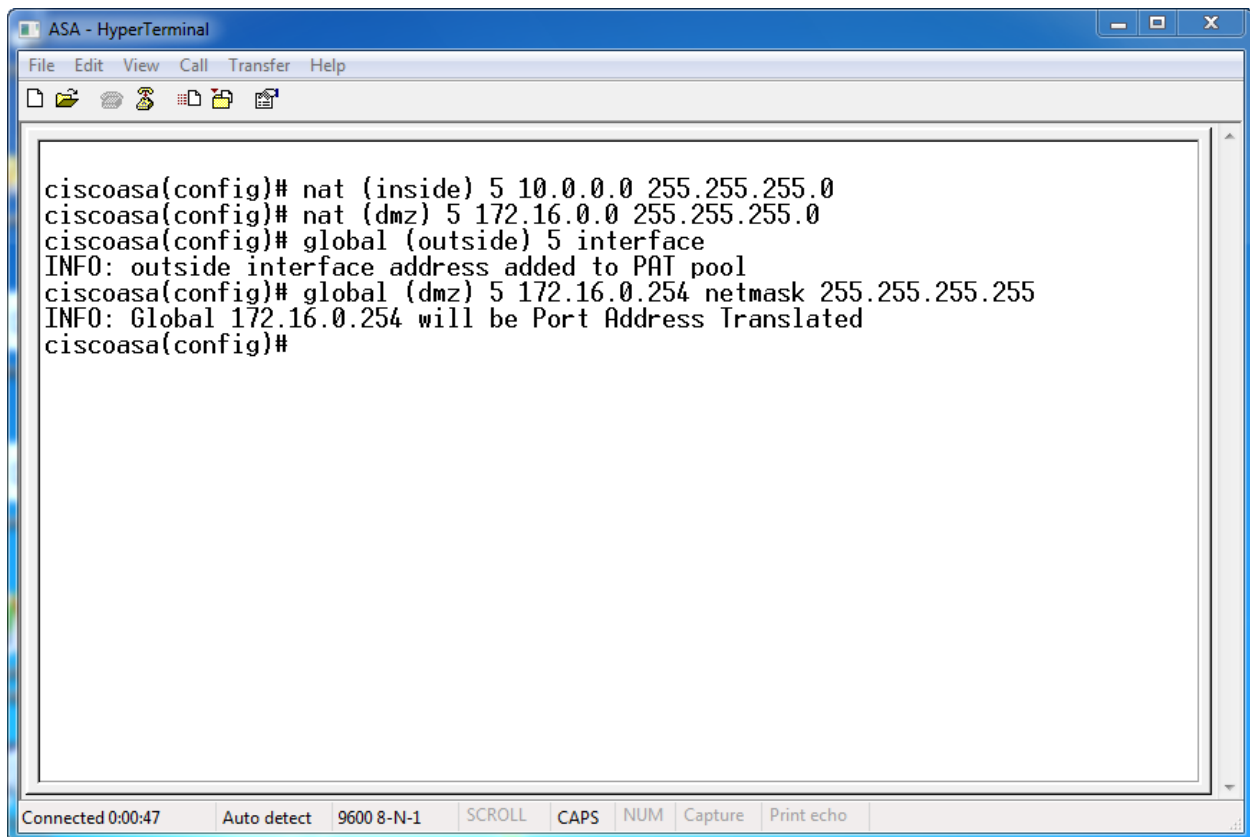
| # | Type | Original | | Translated | | |
|--------------------------|---------|-------------------|-------------|------------|-----------|--------------|
| | | Source | Destination | Service | Interface | Address |
| inside (2 Dynamic rules) | | | | | | |
| 1 | Dynamic | inside-network/24 | | | dmz | 172.16.0.254 |
| 2 | | | | | outside | outside |
| dmz | | | | | | |
| 1 | Dynamic | dmz-network/24 | | | outside | outside |

Enable traffic through the firewall without address translation

Apply Reset

Configuration changes saved successfully.

<admin> 15 4/4/14 9:05:39 AM UTC



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

```
ciscoasa(config)# nat (inside) 5 10.0.0.0 255.255.255.0
ciscoasa(config)# nat (dmz) 5 172.16.0.0 255.255.255.0
ciscoasa(config)# global (outside) 5 interface
INFO: outside interface address added to PAT pool
ciscoasa(config)# global (dmz) 5 172.16.0.254 netmask 255.255.255.255
INFO: Global 172.16.0.254 will be Port Address Translated
ciscoasa(config)#
```

The terminal window has a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. At the bottom of the window, there is a status bar with the following text: "Connected 0:00:47", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Cấu hình Dynamic Inside Policy NAT

The screenshot shows the Cisco ASDM 7.1 for ASA - 192.168.1.1 interface. The main window displays the configuration for a Dynamic Policy NAT rule. The left sidebar shows the configuration tree with 'Firewall' selected. The main area is titled 'Edit Dynamic Policy NAT Rule' and contains the following fields and sections:

- Original:**
 - Interface: inside
 - Source: inside-network/24
 - Destination: 209.165.202.150
 - Source Service: (Optional, TCP or UDP service only)
 - Service: (Optional)
- Translated:**
 - Select a global pool for dynamic translation.
 - Table with columns: Pool ID, Interface, Addresses Pool
 - Row 1: 8, outside, 209.165.200.134
 - Manage... button
- Description:** (Empty text box)
- Connection Settings:** (Dropdown menu)
- Buttons: OK, Cancel, Help

At the bottom of the window, there are 'Apply' and 'Reset' buttons. The status bar at the bottom indicates 'Configuration changes saved successfully.' and shows the user as '<admin>' on page 15, with a timestamp of 4/4/14 9:18:29 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

Firewall

- Access Rules
- NAT Rules**
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Botnet Traffic Filter
- Objects
- Unified Communications
- Advanced
 - Anti-Spoofing
 - Certificate Management
 - Fragment
 - IP Audit
 - SUNRPC Server
 - TCP Options
 - Global Timeouts
 - Virtual Access
 - ACL Manager
 - Standard ACL
 - Per-Session NAT Rules

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

Configuration > Firewall > NAT Rules

+ Add - Edit Delete | Find Diagram Packet Trace

| # | Type | Original | | Translated | | |
|--------|----------------|-------------------|-----------------|------------|-----------|-----------------|
| | | Source | Destination | Service | Interface | Address |
| inside | | | | | | |
| 1 | Dynamic Policy | inside-network/24 | 209.165.202.150 | | outside | 209.165.200.134 |

Enable traffic through the firewall without address translation

Apply Reset

Configuration changes saved successfully.

<admin> 15 4/4/14 9:18:49 AM UTC

```
ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# access-list policy-nat permit ip 10.0.0.0 255.255.255.0 hos$
ciscoasa(config)# nat (inside) 8 access-list policy-nat
ciscoasa(config)# global (outside) 8 209.165.202.134 netmask 255.255.255.255
INFO: Global 209.165.202.134 will be Port Address Translated
ciscoasa(config)#
Connected 0:00:36 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Cấu hình STATIC INSIDE NAT

The screenshot displays the Cisco ASDM 7.1 for ASA interface. The main window is titled "Configuration > Firewall > NAT Rules". A dialog box titled "Add Static NAT Rule" is open, showing the following configuration:

- Original:**
 - Interface: dmz
 - Source: 10.0.0.5
- Translated:**
 - Interface: outside
 - Use IP Address: 209.165.200.228
 - Use Interface IP Address
- Port Address Translation (PAT):**
 - Enable Port Address Translation (PAT)
 - Protocol: TCP UDP
 - Original Port:
 - Translated Port:

At the bottom of the dialog box, there are "OK", "Cancel", and "Help" buttons. Below the dialog box, in the main configuration area, there is a checkbox for "Enable traffic through the firewall without address translation" which is currently unchecked. At the bottom of the main window, there are "Apply" and "Reset" buttons. The status bar at the bottom of the window shows "Configuration changes saved successfully.", the user is logged in as "<admin>", and the date/time is "4/4/14 9:33:09 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

Firewall

- Access Rules
- NAT Rules**
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- 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

| # | Type |
|---|--------|
| 1 | Static |

Add Static NAT Rule

Original

Interface: dmz

Source: 172.16.0.10

Translated

Interface: outside

Use IP Address: 209.165.200.229

Use Interface IP Address

Port Address Translation (PAT)

Enable Port Address Translation (PAT)

Protocol: TCP UDP

Original Port:

Translated Port:

Connection Settings

OK Cancel Help

Address

| Address |
|-----------------|
| 209.165.200.228 |

Enable traffic through the firewall without address translation

Apply Reset

Device configuration refreshed successfully.

<admin> 15 4/4/14 9:40:09 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
- 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

| # | Type | Original | | Translated | | |
|----------------------|--------|-------------|-------------|------------|-----------|-----------------|
| | | Source | Destination | Service | Interface | Address |
| dmz (2 Static rules) | | | | | | |
| 1 | Static | 172.16.0.5 | | | outside | 209.165.200.228 |
| 2 | Static | 172.16.0.10 | | | outside | 209.165.200.229 |

Enable traffic through the firewall without address translation

Apply Reset

Device configuration refreshed successfully.

<admin> 15 4/4/14 9:40:29 AM UTC

```
ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# static (dmz,outside) 209.165.200.228 172.16.0.5 netmask 255.$
ciscoasa(config)# static (dmz,outside) 209.165.200.229 172.16.0.10 netmask 255$
ciscoasa(config)# _
|
Connected 0:02:53 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Cấu hình NETWORK STATIC INSIDE NAT

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Firewall > NAT Rules". A dialog box titled "Add Static NAT Rule" is open, showing the following configuration:

- Original:**
 - Interface: dmz
 - Source: 172.16.0.32/27
- Translated:**
 - Interface: outside
 - Use IP Address: 209.165.201.0/27
 - Use Interface IP Address
- Port Address Translation (PAT):**
 - Enable Port Address Translation (PAT)
 - Protocol: TCP UDP
 - Original Port:
 - Translated Port:

At the bottom of the dialog box, there are "OK", "Cancel", and "Help" buttons. Below the dialog box, in the main configuration area, there is a checkbox for "Enable traffic through the firewall without address translation" which is currently unchecked. At the bottom of the main window, there are "Apply" and "Reset" buttons. The status bar at the bottom of the window shows "Configuration changes saved successfully.", the user is logged in as "<admin>", and the date and time are "4/4/14 9:43:49 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

Firewall

- Access Rules
- NAT Rules**
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- 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

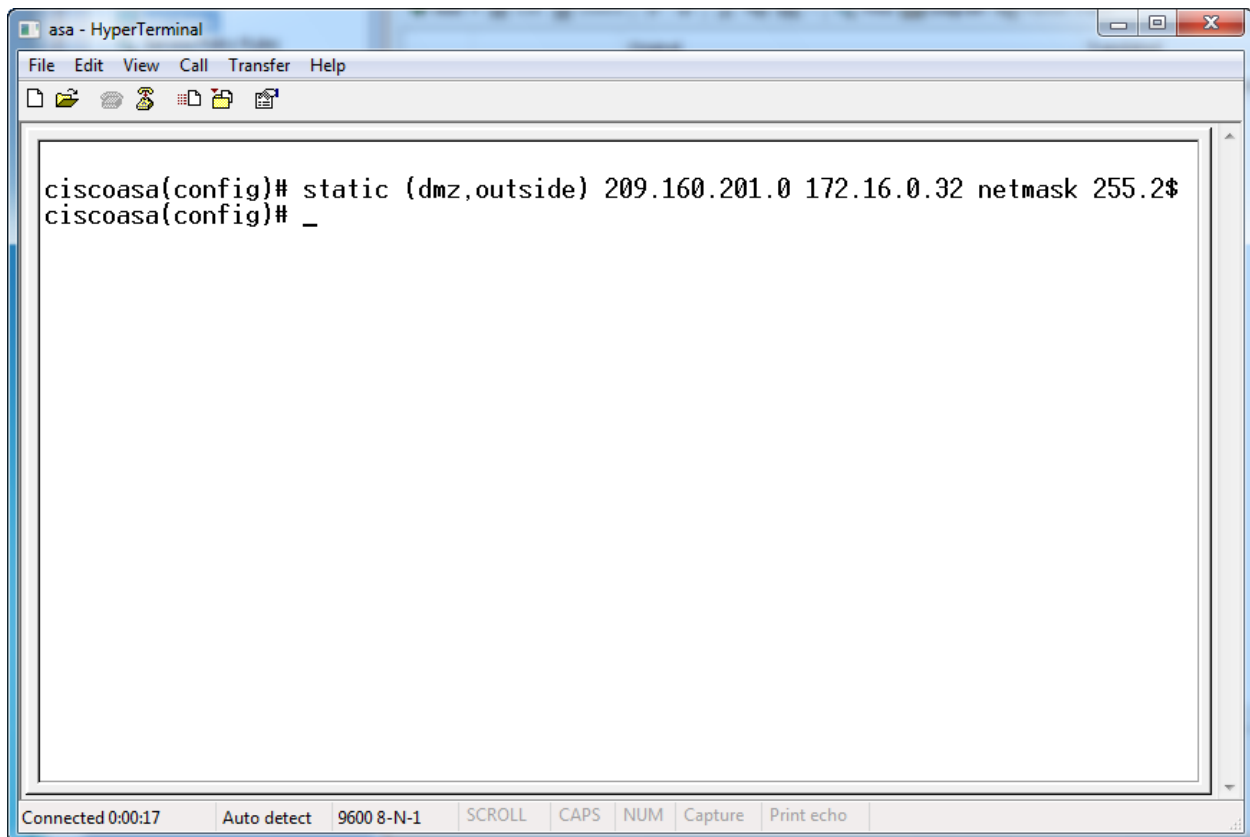
| # | Type | Original | | Translated | | |
|-----|--------|----------------|-------------|------------|-----------|------------------|
| | | Source | Destination | Service | Interface | Address |
| dmz | | | | | | |
| 1 | Static | 172.16.0.32/27 | | | outside | 209.165.201.0/27 |

Enable traffic through the firewall without address translation

Apply Reset

Configuration changes saved successfully.

<admin> 15 4/4/14 9:44:09 AM UTC



The image shows a HyperTerminal window titled "asa - HyperTerminal". The window contains a command prompt for a Cisco ASA device in configuration mode. The command entered is "static (dmz,outside) 209.160.201.0 172.16.0.32 netmask 255.255.255.0", which is partially visible as "255.2\$". The prompt returns to the configuration mode prompt "ciscoasa(config)# _".

```
ciscoasa(config)# static (dmz,outside) 209.160.201.0 172.16.0.32 netmask 255.2$
ciscoasa(config)# _
```

At the bottom of the window, the status bar shows "Connected 0:00:17", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Cấu hình STATIC INSIDE PAT

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Firewall > NAT Rules". A dialog box titled "Add Static NAT Rule" is open, showing the following configuration:

- Original:**
 - Interface: dmz
 - Source: 172.16.0.15
- Translated:**
 - Interface: outside
 - Use IP Address: 209.160.200.230
 - Use Interface IP Address
- Port Address Translation (PAT):**
 - Enable Port Address Translation (PAT)
 - Protocol: TCP UDP
 - Original Port: 8443
 - Translated Port: 443

At the bottom of the dialog box, there are "OK", "Cancel", and "Help" buttons. Below the dialog box, in the main configuration area, there is a checkbox for "Enable traffic through the firewall without address translation" which is currently unchecked. At the bottom of the main window, there are "Apply" and "Reset" buttons.

Configuration changes saved successfully.

<admin> 15 4/4/14 9:52:39 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

Device List

- Firewall
 - Access Rules
 - NAT Rules
 - Service Policy Rules
 - AAA Rules
 - Filter Rules
 - Public Servers
 - URL Filtering Servers
 - Threat Detection
 - 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

Type

| # | Type | Translated Interface | Address |
|---|------|----------------------|-----------------|
| 1 | | dmz | 209.160.200.230 |

Add Static NAT Rule

Original

Interface: dmz

Source: 172.16.0.20

Translated

Interface: outside

Use IP Address: 209.160.200.230

Use Interface IP Address

Port Address Translation (PAT)

Enable Port Address Translation (PAT)

Protocol: TCP UDP

Original Port: 25

Translated Port: 25

Connection Settings

OK Cancel Help

Enable traffic through the firewall without address translation

Apply Reset

Configuration changes saved successfully.

<admin> 15

4/4/14 9:53:59 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
- 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

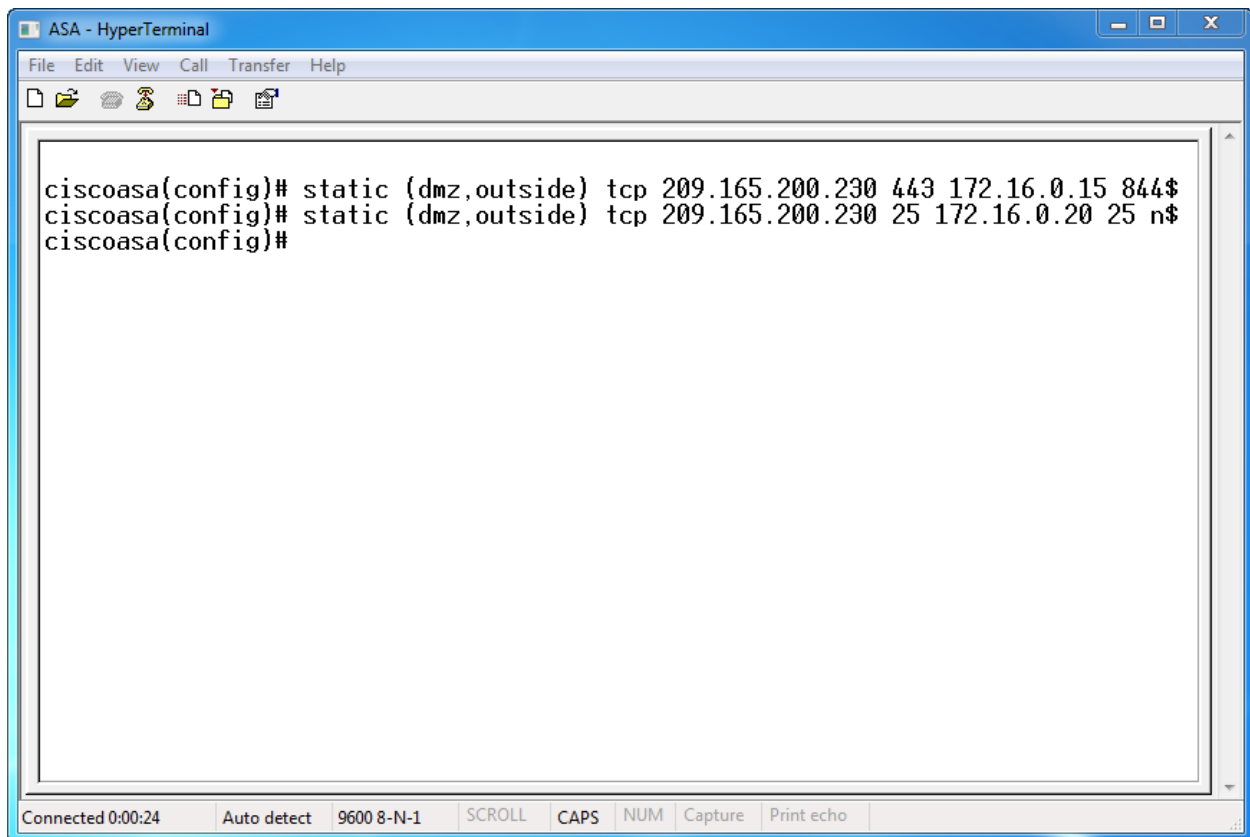
| # | Type | Original | | Translated | | |
|-----|--------|-------------|-------------|------------|-----------|-----------------|
| | | Source | Destination | Service | Interface | Address |
| dmz | | | | | | |
| 1 | Static | 172.16.0.15 | | 8443 | outside | 209.160.200.230 |
| 2 | Static | 172.16.0.20 | | smtp | outside | 209.160.200.230 |

Enable traffic through the firewall without address translation

Apply Reset

Configuration changes saved successfully.

<admin> 15 4/4/14 9:54:29 AM UTC



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

```
ciscoasa(config)# static (dmz,outside) tcp 209.165.200.230 443 172.16.0.15 844$
ciscoasa(config)# static (dmz,outside) tcp 209.165.200.230 25 172.16.0.20 25 n$
ciscoasa(config)#
```

The terminal window includes a menu bar (File, Edit, View, Call, Transfer, Help), a toolbar with icons for file operations, and a status bar at the bottom with the following information: Connected 0:00:24, Auto detect, 9600 8-N-1, SCROLL, CAPS, NUM, Capture, Print echo.

Cấu hình static inside policy nat

The screenshot displays the Cisco ASDM 7.1 for ASA interface. The main window shows the configuration tree on the left with 'NAT Rules' selected. A dialog box titled 'Add Static Policy NAT Rule' is open in the center. The dialog is divided into several sections:

- Original:** Interface: ; Source: ; Destination:
- Translated:** Interface: ; Use IP Address: ; Use Interface IP Address
- Port Address Translation (PAT):** Enable Port Address Translation (PAT); Protocol: TCP UDP; Original Port: ; Translated Port:
- Description:**
- Connection Settings:**

At the bottom of the dialog are buttons for 'OK', 'Cancel', and 'Help'. Below the dialog, in the main window, are 'Apply' and 'Reset' buttons. The status bar at the bottom of the ASDM window shows 'Configuration changes saved successfully.', the user '<admin>', the page number '15', and the date/time '4/4/14 10:03:09 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

Firewall

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

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

Configuration > Firewall > NAT Rules

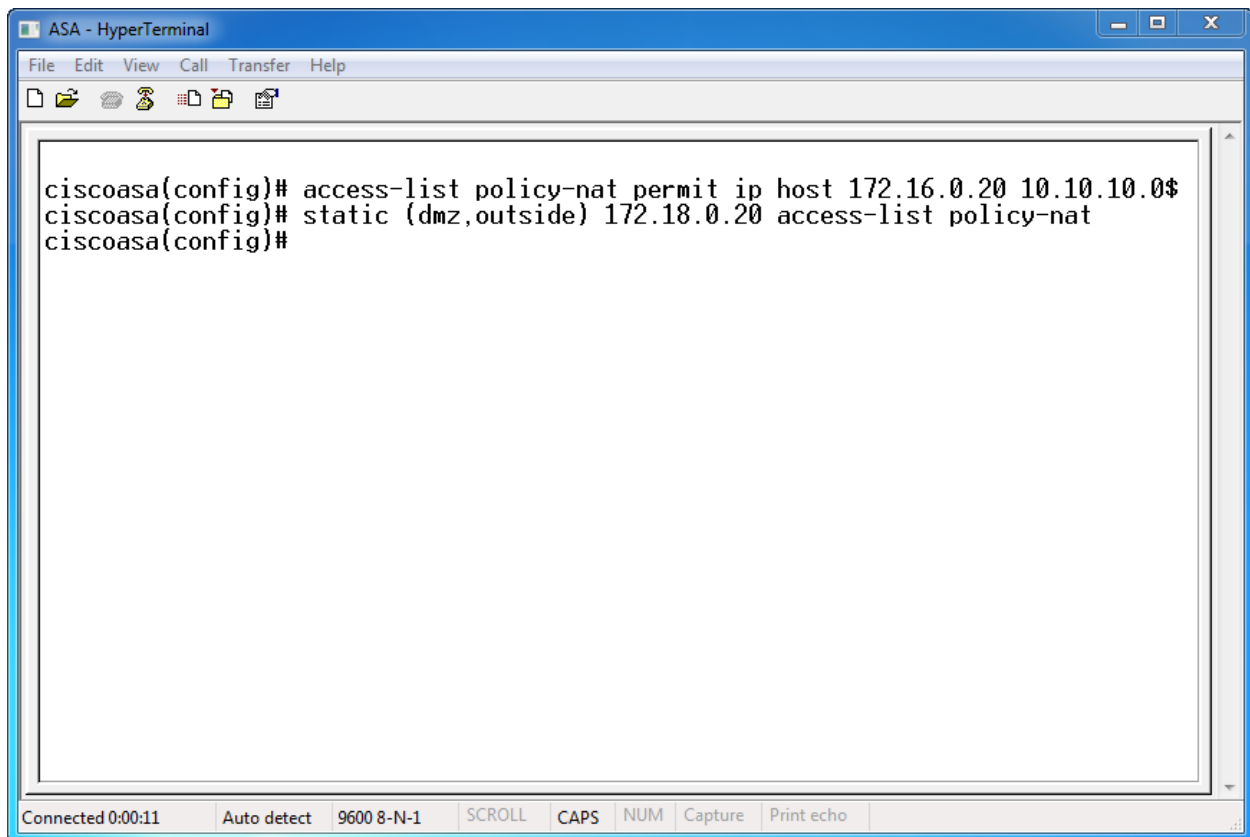
+ Add - Edit Delete Find Diagram Packet Trace

| # | Type | Original | | Translated | | |
|---|---------------|-------------|---------------|------------|-----------|-------------|
| | | Source | Destination | Service | Interface | Address |
| 1 | Static Policy | 172.16.0.20 | 10.10.10.0/24 | | outside | 172.18.0.20 |

Enable traffic through the firewall without address translation

Apply Reset

Configuration changes saved successfully. <admin> 15 4/4/14 10:03:39 AM UTC



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

```
ciscoasa(config)# access-list policy-nat permit ip host 172.16.0.20 10.10.10.0$
ciscoasa(config)# static (dmz,outside) 172.18.0.20 access-list policy-nat
ciscoasa(config)#
```

The bottom status bar of the window displays the following information: "Connected 0:00:11", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Cấu hình DYNAMIC IDENTITY NAT

The screenshot shows the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Firewall > NAT Rules". A dialog box titled "Add Dynamic NAT Rule" is open in the foreground. The dialog box has two sections: "Original" and "Translated".

Original Section:

- Interface: inside
- Source: inside-network/24

Translated Section:

Select a global pool for dynamic translation.

| Pool ID | Interface | Addresses Pool |
|---------|------------|-------------------------------------|
| 0 | (outbound) | Same as original address (identity) |
| -0 | (inbound) | Same as original address (identity) |

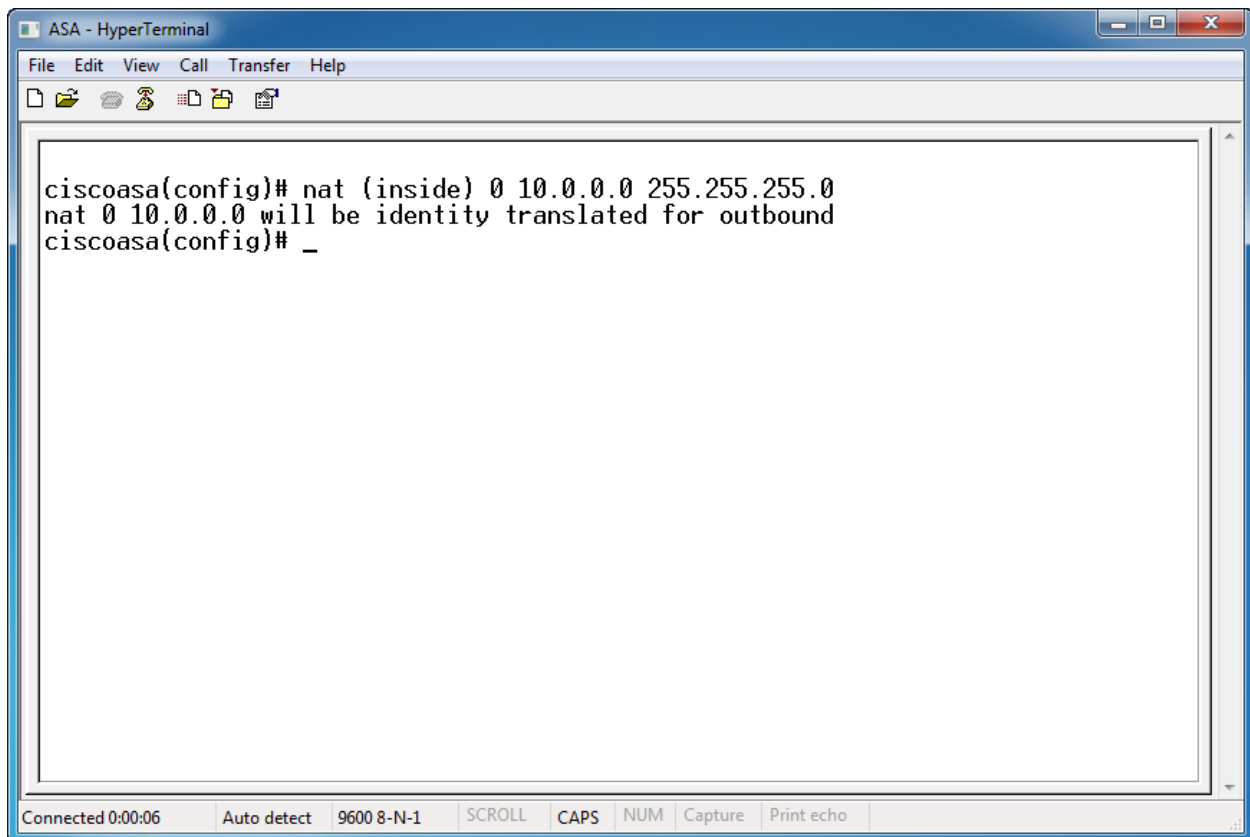
Buttons: Manage...

Connection Settings

Buttons: OK, Cancel, Help

At the bottom of the dialog box, there is a checkbox labeled "Enable traffic through the firewall without address translation" which is currently unchecked. Below this checkbox are "Apply" and "Reset" buttons.

The background interface shows a left-hand navigation pane with "Firewall" selected. The main pane shows a table with columns for "#", "Type", "Original", and "Translated". The status bar at the bottom indicates "Configuration changes saved successfully." and the user is logged in as "<admin>" on page 15. The system time is 4/4/14 10:14:39 AM UTC.



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

```
ciscoasa(config)# nat (inside) 0 10.0.0.0 255.255.255.0
nat 0 10.0.0.0 will be identity translated for outbound
ciscoasa(config)# _
```

The bottom status bar of the window displays the following information: "Connected 0:00:06", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Cấu hình STATIC IDENTITY NAT

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Firewall > NAT Rules". A dialog box titled "Add Static NAT Rule" is open, showing the following configuration:

- Original:**
 - Interface:
 - Source:
- Translated:**
 - Interface:
 - Use IP Address:
 - Use Interface IP Address
- Port Address Translation (PAT):**
 - Enable Port Address Translation (PAT)
 - Protocol: TCP UDP
 - Original Port:
 - Translated Port:

At the bottom of the dialog box, there are "OK", "Cancel", and "Help" buttons. Below the dialog box, in the main configuration area, there is a checkbox for "Enable traffic through the firewall without address translation" which is currently unchecked. At the bottom of the main window, there are "Apply" and "Reset" buttons. The status bar at the bottom of the window shows "Configuration changes saved successfully.", the user role "<admin>", the page number "15", and the date/time "4/4/14 10:19:19 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
- 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

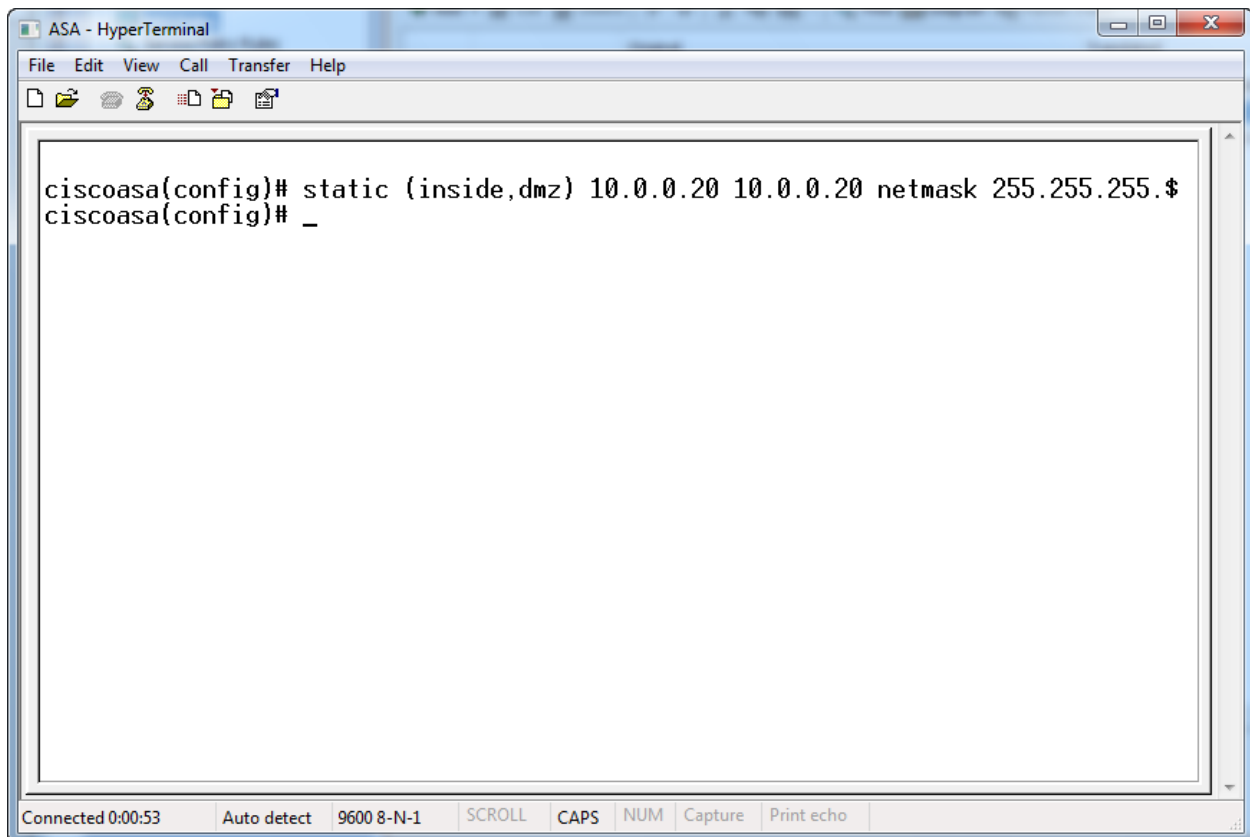
| # | Type | Original | | Translated | | |
|-------------------------|--------|-----------|-------------|------------|-----------|-----------|
| | | Source | Destination | Service | Interface | Address |
| inside (1 Static rules) | | | | | | |
| 1 | Static | 10.0.0.20 | | | dmz | 10.0.0.20 |

Enable traffic through the firewall without address translation

Apply Reset

Device configuration refreshed successfully.

<admin> 15 4/4/14 10:20:59 AM UTC



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window has a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. The main area of the window displays a command-line interface for a Cisco ASA device. The prompt is "ciscoasa(config)#". The command entered is "static (inside,dmz) 10.0.0.20 10.0.0.20 netmask 255.255.255.255". The prompt is followed by a dollar sign "\$" on the next line, and then an underscore "_" on the following line. The status bar at the bottom of the window shows "Connected 0:00:53", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

```
ciscoasa(config)# static (inside,dmz) 10.0.0.20 10.0.0.20 netmask 255.255.255.$
ciscoasa(config)# _
```

Connected 0:00:53 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Cấu hình NAT BYPASS (NAT EXEMPTION)

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Firewall > NAT Rules". A dialog box titled "Add NAT Exempt Rule" is open, showing the following configuration:

- Action:** Exempt Do not exempt
- Original:**
 - Interface: inside
 - Source: inside-network/24
 - Destination: dmz-network/24
- NAT Exempt Direction:**
 - NAT Exempt outbound traffic from interface 'inside' to lower security interfaces (default)
 - NAT Exempt inbound traffic from interface 'inside' to higher security interfaces
- Description:** (Empty text box)

At the bottom of the dialog, there are "OK", "Cancel", and "Help" buttons. Below the dialog, in the main configuration area, there is a checkbox for "Enable traffic through the firewall without address translation" which is currently unchecked. "Apply" and "Reset" buttons are also visible.

At the bottom of the ASDM window, a status bar shows "Configuration changes saved successfully." on the left, and on the right, it displays the user "`<admin>`", the page number "15", and the date/time "4/4/14 10:26:39 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
- 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

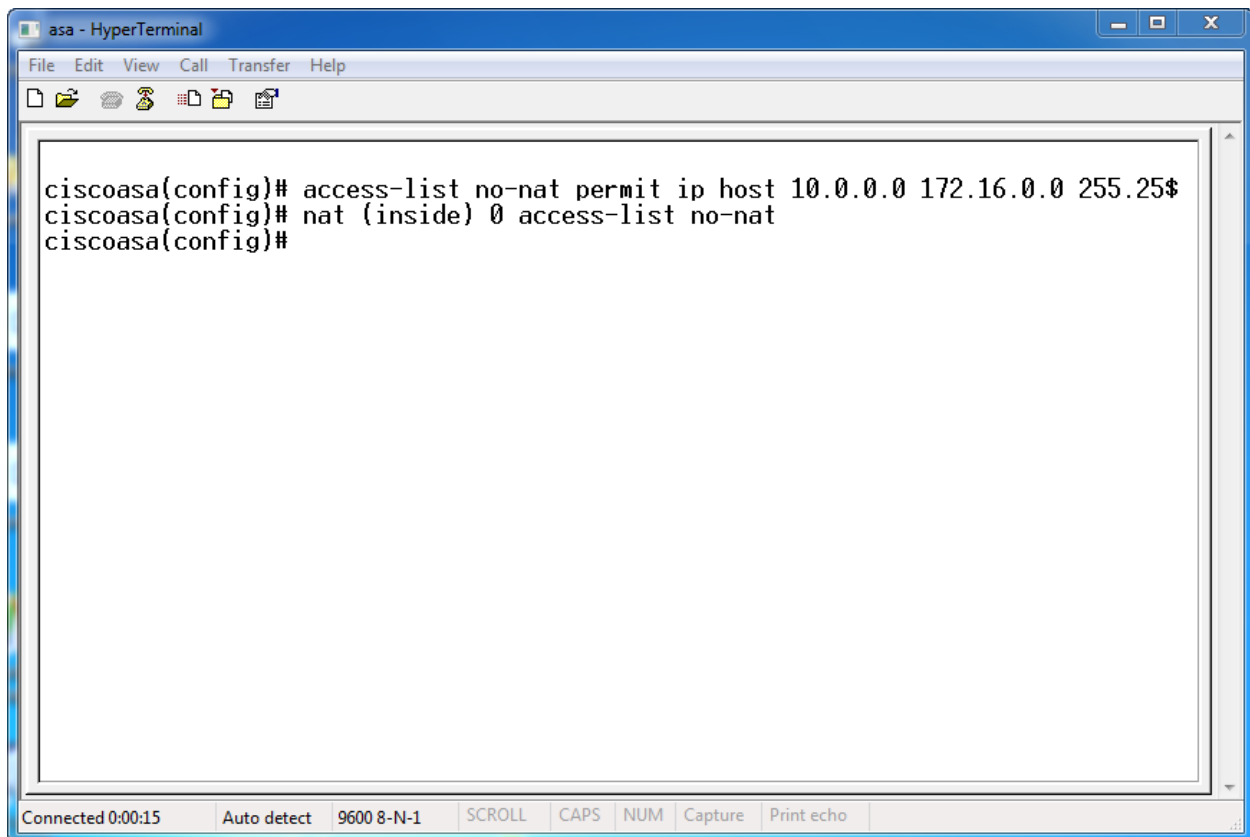
| # | Type | Original | | Translated | | |
|--------|--------|-------------------|----------------|------------|-------------------|--|
| | | Source | Destination | Service | Interface Address | |
| inside | | | | | | |
| 1 | Exempt | inside-network/24 | dmz-network/24 | | (outbound) | |

Enable traffic through the firewall without address translation

Apply Reset

Configuration changes saved successfully.

<admin> 15 4/4/14 10:27:09 AM UTC



The image shows a HyperTerminal window titled "asa - HyperTerminal". The window contains a terminal session with the following commands and output:

```
ciscoasa(config)# access-list no-nat permit ip host 10.0.0.0 172.16.0.0 255.255.255.255
ciscoasa(config)# nat (inside) 0 access-list no-nat
ciscoasa(config)#
```

The status bar at the bottom of the window displays: "Connected 0:00:15", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

