



# NAT și lucrul avansat cu ACL-uri

19 martie 2015

# Obiective

---

- ▶ Ce este NAT
- ▶ Tipuri de translații
- ▶ Tipurile de NAT configurabile pe ASA
- ▶ Scenarii de implementare
- ▶ Nat-control
- ▶ Modalități de bypass NAT
- ▶ Lucrul avansat cu ACL-uri

# Ce este NAT?

---

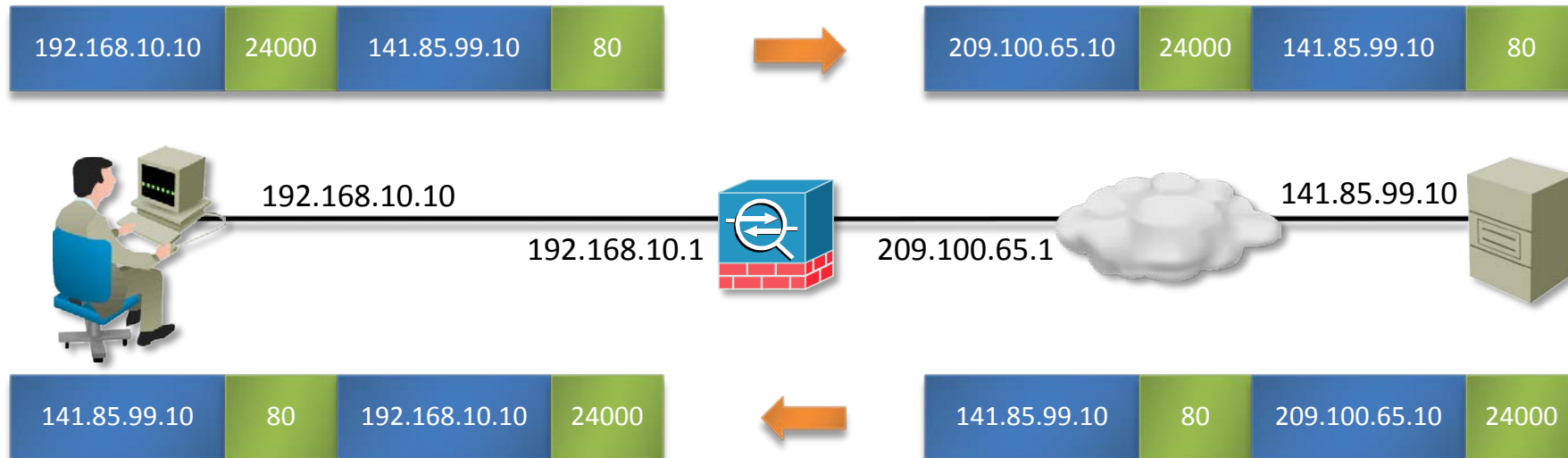
- ▶ NAT definește modul în care translatăm adrese private în adrese publice și invers

## Welcome to NAT Trivia!!!

- ▶ Care sunt adresele private?
  - ❑ Clasa A: 10.0.0.0/8: **16,777,214** hosturi
  - ❑ Clasa B: 172.16.0.0/12: **1,048,574** hosturi
  - ❑ Clasa C: 192.168.0.0/16: **65,534** hosturi
- ▶ Adresele private sunt definite în RFC 1918.
- ▶ Funcție de nivelul din stiva OSI la care se operează există 2 tipuri de translație:
  - ❑ NAT (Network Address Translation) – nivelul 3
  - ❑ PAT (Port Address Translation) – nivelul 4

# NAT – Inside NAT

- ▶ Funcție de direcția în care se face translatarea:
  - ❑ Inside NAT – adresele din LAN sunt translatate la adrese din WAN
  - ❑ Outside NAT – adresele din WAN sunt translatate la adrese din LAN
- ▶ Inside NAT

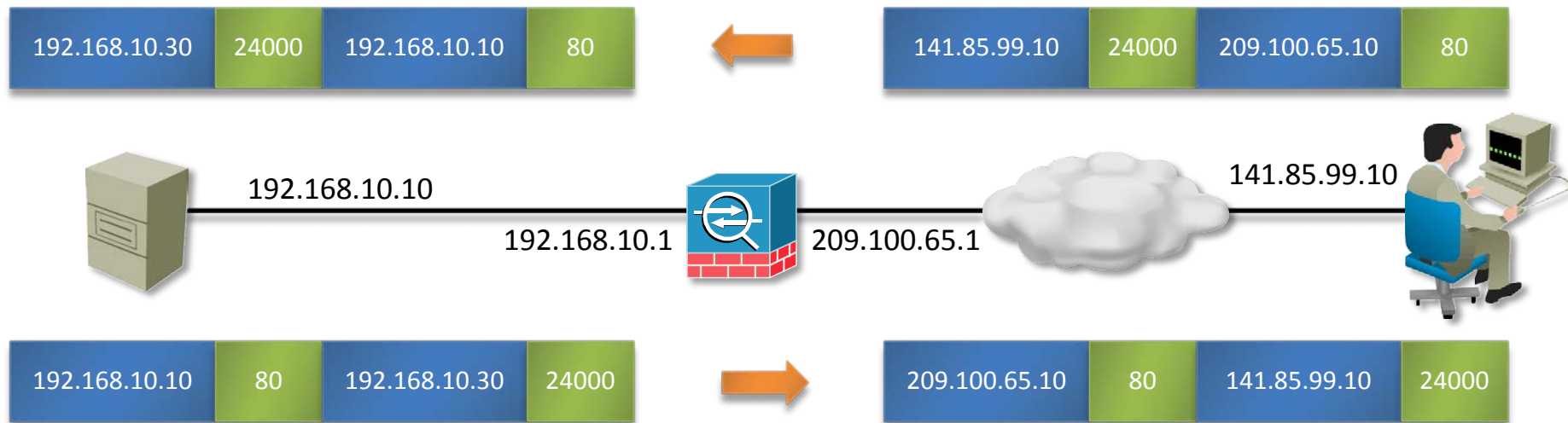


- ▶ Firewall-ul modifică doar antetul de nivel 3 pentru a face NAT
- ▶ De obicei se folosesc adrese din același pool public pentru NAT și pentru adresa de pe interfața de outside a ASA

# NAT – Outside NAT

## ► Outside NAT

- ❑ este de fapt NAT bidirecțional
- ❑ se traduce adresa sursă a pachetelor ce vin din extern



- Folosit în cazul în care se dorește ca hosturile din exterior să pară că sunt în interiorul rețelei

# Mituri NAT

---



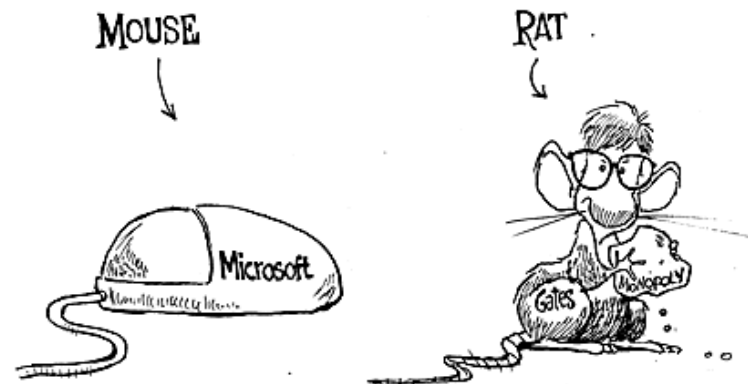
- ▶ “NAT conservă adrese”
  - ❑ Fiecare adresa privată este translatată într-o unică adresă publică
- ▶ “NAT este un mecanism de securitate”
  - ❑ Funcționalitatea de securitatea rețelei din NAT este o consecință, nu un obiectiv al designului
  - ❑ Nu este de obicei recomandat designul securității inside-outside pe baza NAT
  - ❑ Există alt dispozitiv care din punct de vedere al securității îndeplinește aceeași funcție ca NAT: **stateful firewall**
  - ❑ Un stateful firewall are și funcții suplimentare (Application Inspection etc.)
- ▶ Totuși, la nivel psihologic, NAT este considerat un mecanism de securitate de multe companii
  - ❑ Unul din motivele puternice pentru care există adrese private în IPv6

# Terminologie NAT

---

- ▶ Atenție la terminologia NAT, este destul de diversă.
  - ❑ Ce este SNAT?
    - Inside NAT
  - ❑ Ce este DNAT?
    - Un concept numit port-forwarding/port-redirection, nu outside NAT

## Terminology



# PAT

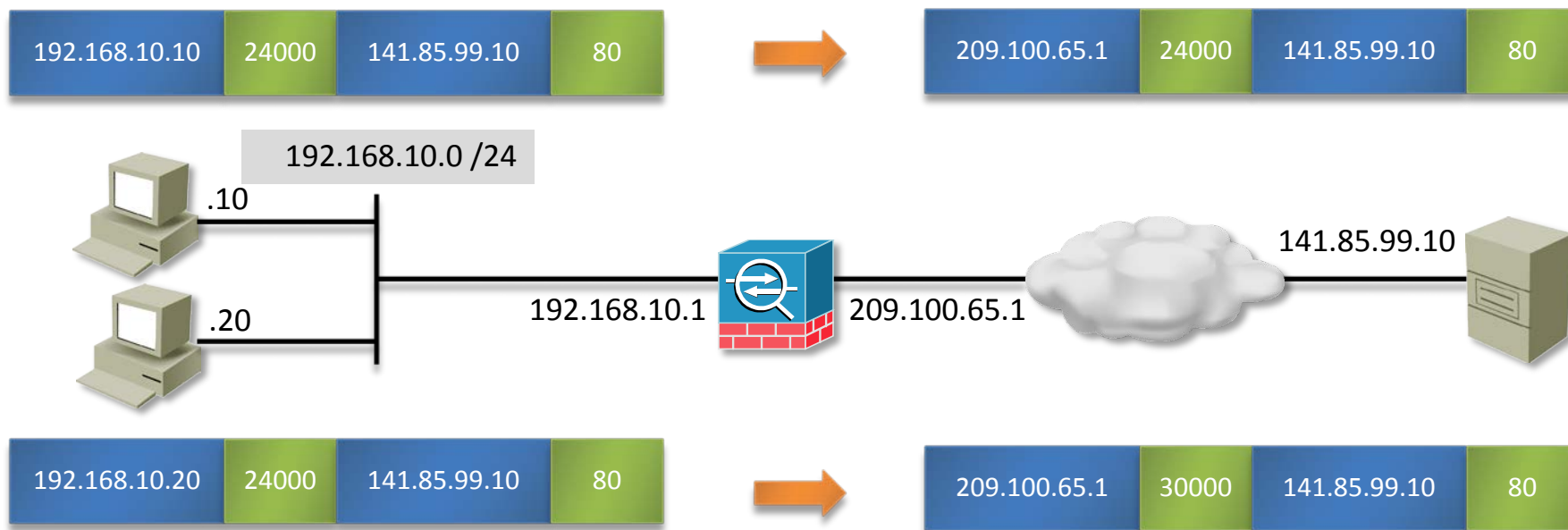
---

- ▶ Port address translation
  - ❑ Permite translatarea de foarte multe adrese private, folosind o singură adresă publică
- ▶ Pentru că nu se mai poate face mapare 1-1 la nivel 3, se face la nivel 4
- ▶ Fiecare pereche (IP\_intern, port\_intern) este mapată la (IP\_extern, port\_extern)
- ▶ În mod implicit procesul de PAT va încerca să mapeze portul intern pe același port extern
  - ❑ Dacă portul extern a fost însă mapat la o translatare anterioară, se mapează pe un port random
- ▶ Mapările PAT se rețin în memoria firewall-ului și sunt folosite pentru a identifica traficul de întoarcere și a îl translata înapoi



# Exemplu de funcționare

- ▶ Pentru adresa translatată se poate folosi:
  - ❑ Adresa de pe interfața fizică
  - ❑ O adresă publică nealocată pe o interfață fizică



- ▶ Pentru protocoalele connection-oriented, firewall-ul șterge translatarea din memorie odată cu încheierea conexiunii
- ▶ Pentru protocoalele connectionless fiecare intrare are un timeout

# Connection vs Translation

---

- ▶ Atenție, cele două sunt concepte diferite pentru un firewall
- ▶ Scenariu: un utilizator descarcă o pagina web, transmite IM cu un prieten și descarcă mailurile în clientul de mail.
- ▶ Câte conexiuni reține firewall-ul în memorie?
  - ❑ 3 (posibil mai multe funcție de protocoalele folosite)
- ▶ Câte translatări NAT(nivel 3) reține firewall-ul în memorie?
  - ❑ 1



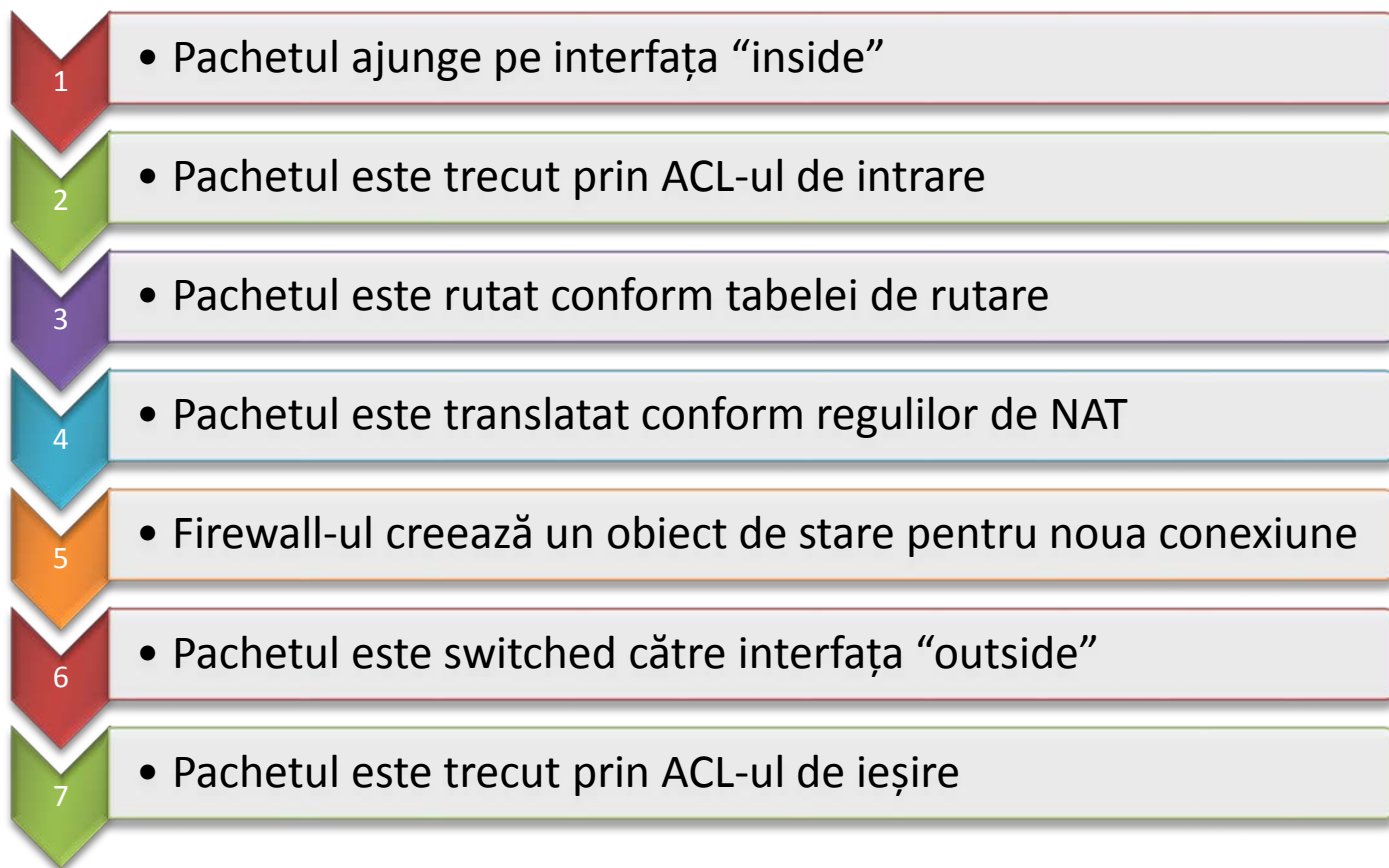


# Configurații NAT pe Cisco ASA

# Procesarea pachetelor - inside

---

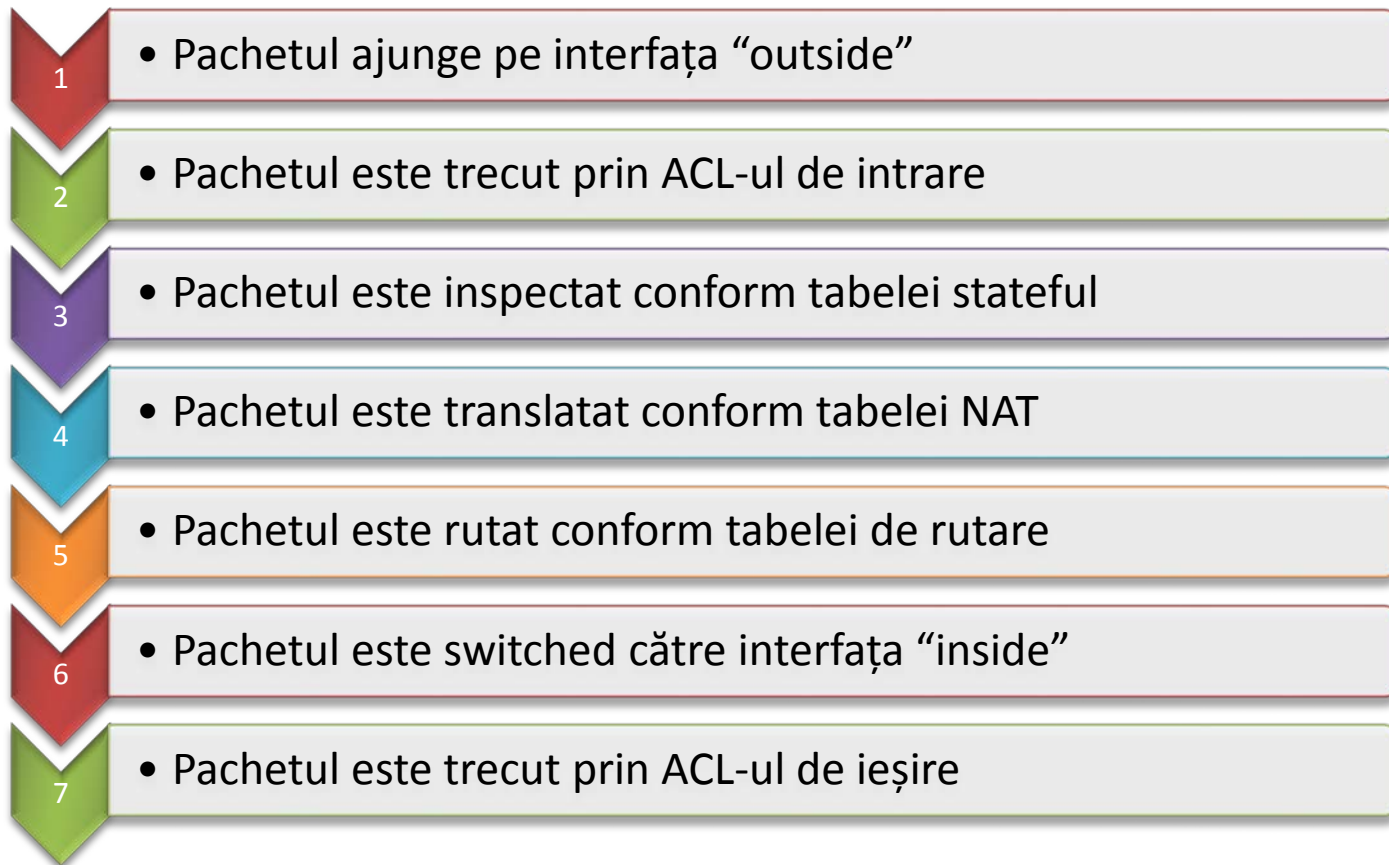
- Ordinea operațiilor de mai jos este realizată pentru ASA OS 8.0 (versiunea folosită în laborator)



# Procesarea pachetelor - outside

---

- Ordinea operațiilor de mai jos este realizată pentru ASA OS 8.0 (versiunea folosită în laborator)



## ASA OS 8.3 – Real IP

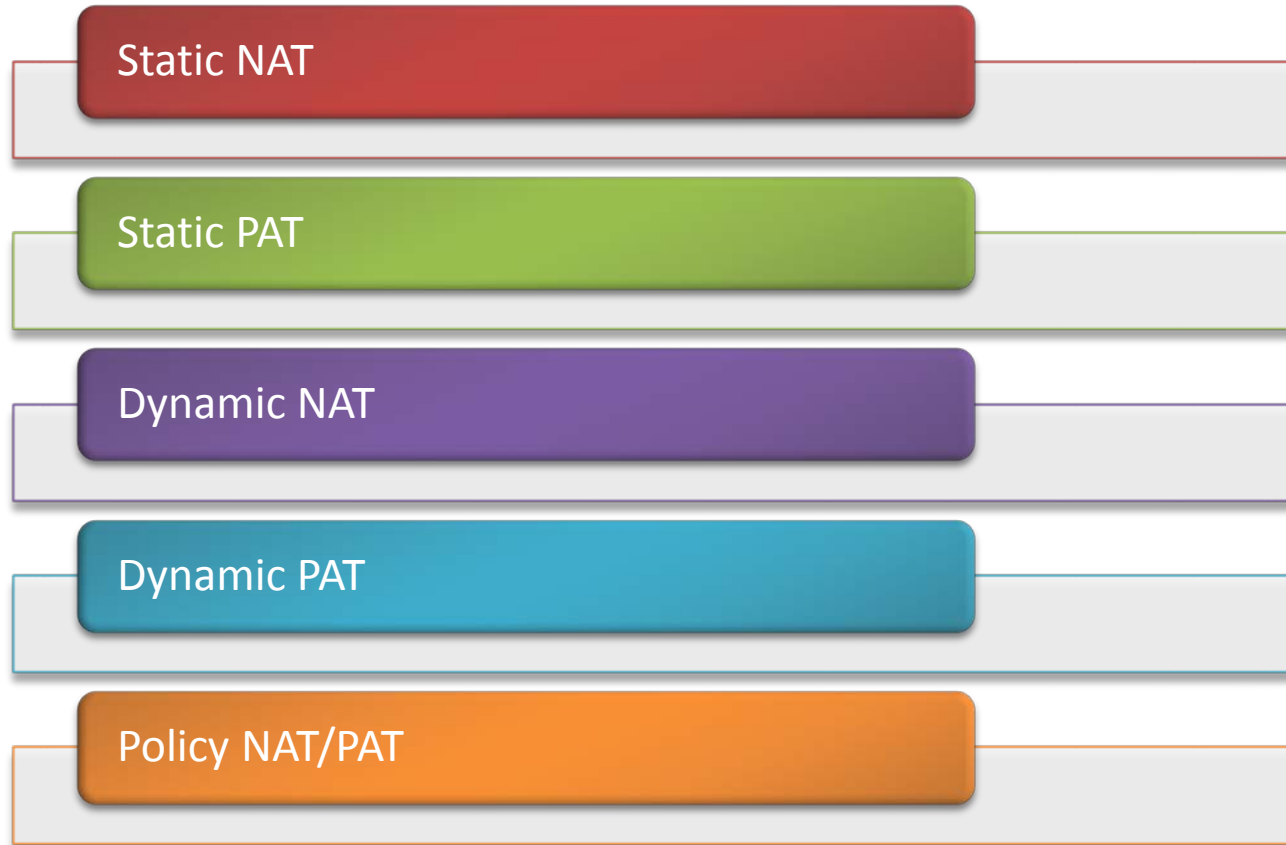
---

- ▶ Noua versiune 8.3 a introdus un feature numit “Real IP”
- ▶ Problema: dacă se schimbă ceva în politicile NAT trebuie ca administratorul să schimbe și celelalte politici de firewall (ACL-uri, application inspection etc.)
- ▶ În 8.3, ASA realizează NAT înainte de procesarea ACL-ului de pe interfața pe care intră pachetul
- ▶ Astfel administratorul poate defini ACL-urile și alte configurații direct cu IP-urile reale din LAN

# Tipuri de NAT

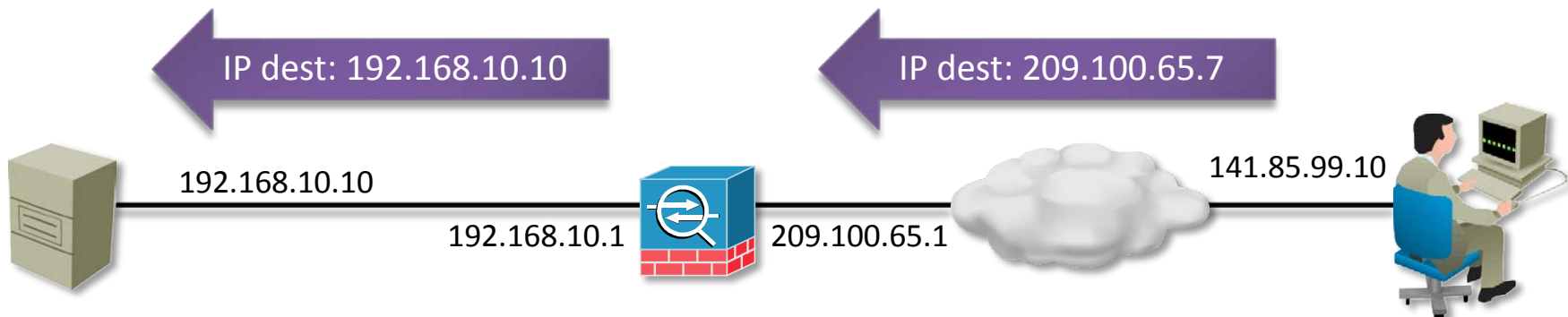
---

- ▶ ASA definește 5 tipuri de NAT:



# Static NAT

- ▶ Un IP privat este întotdeauna tradus în același IP public
- ▶ Intrarea în tabela NAT este statică (nu face age-out)
- ▶ În ce scenariu avem nevoie de Static NAT?



- ❑ Când avem un server în DMZ cu adresă privată, ce trebuie accesat din exterior oricând, cu aceeași adresa publică

```
Waters(config)# static (inside,outside) 209.100.65.7  
192.168.10.10 netmask 255.255.255.255
```



# Static NAT – setări avansate

---

- ▶ Comanda **static** suportă și setarea limitelor de conexiune TCP/UDP pentru pachetele translatate
  - ❑ Comanda de mai jos setează numărul de conexiuni TCP și UDP la 1000 și numărul de conexiuni embryonic la 100

```
Waters(config)# static (inside,outside) 209.100.65.7  
192.168.10.10 netmask 255.255.255.255 tcp 1000 100 udp 1000
```

# Static NAT – setări avansate

---

- ▶ Comanda de mai jos elimină funcționalitate de randomizare a ISN-ului unei conexiuni

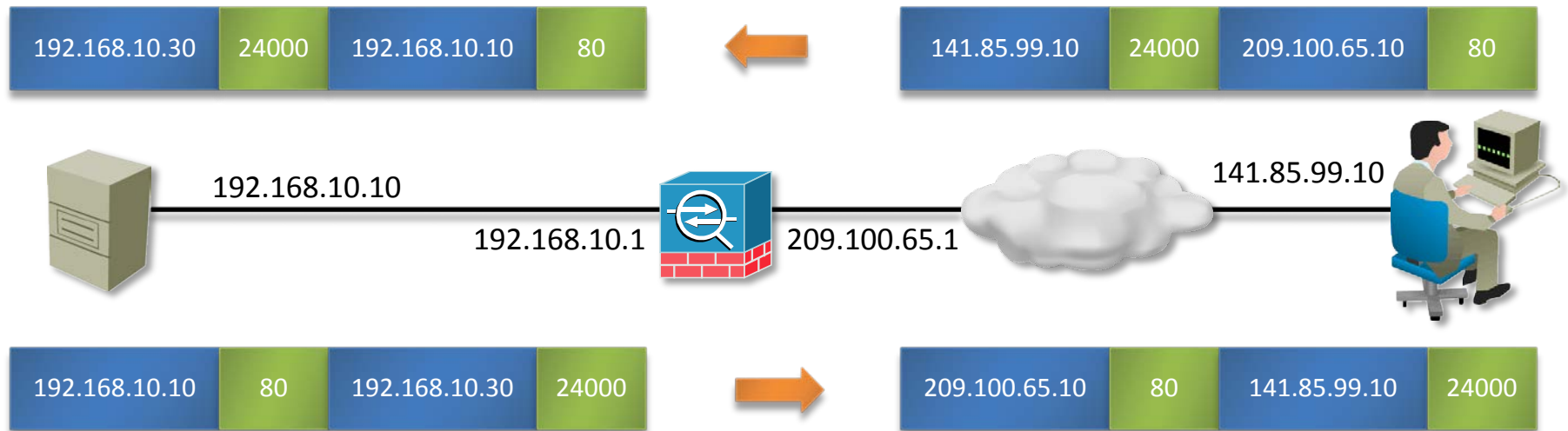
```
Waters(config)# static (inside,outside) 89.141.99.1 89.141.99.1  
netmask 255.255.255.255 norandomseq
```

- ▶ Când ar fi util dezactivarea acesteia?
  - ❑ Când funcționează o schemă de autentificare ce folosește MD5 (BGP)

# Outside NAT

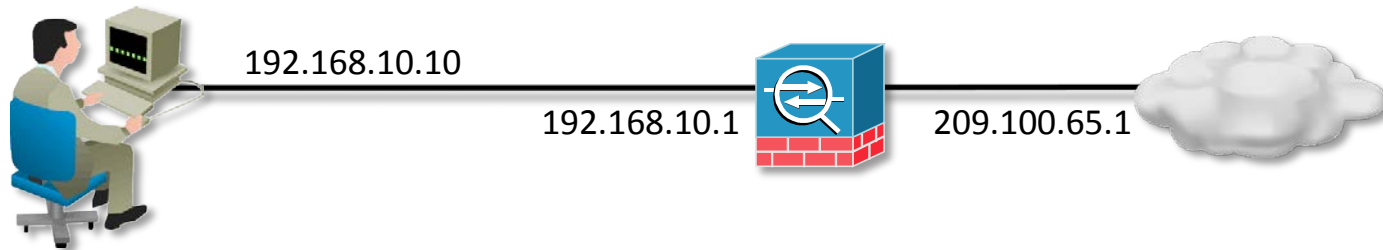
- Comanda static poate fi folosită și pentru outside NAT

```
Waters(config)# static (outside,inside) 192.168.10.30  
209.100.65.10 netmask 255.255.255.255
```



# Dynamic NAT

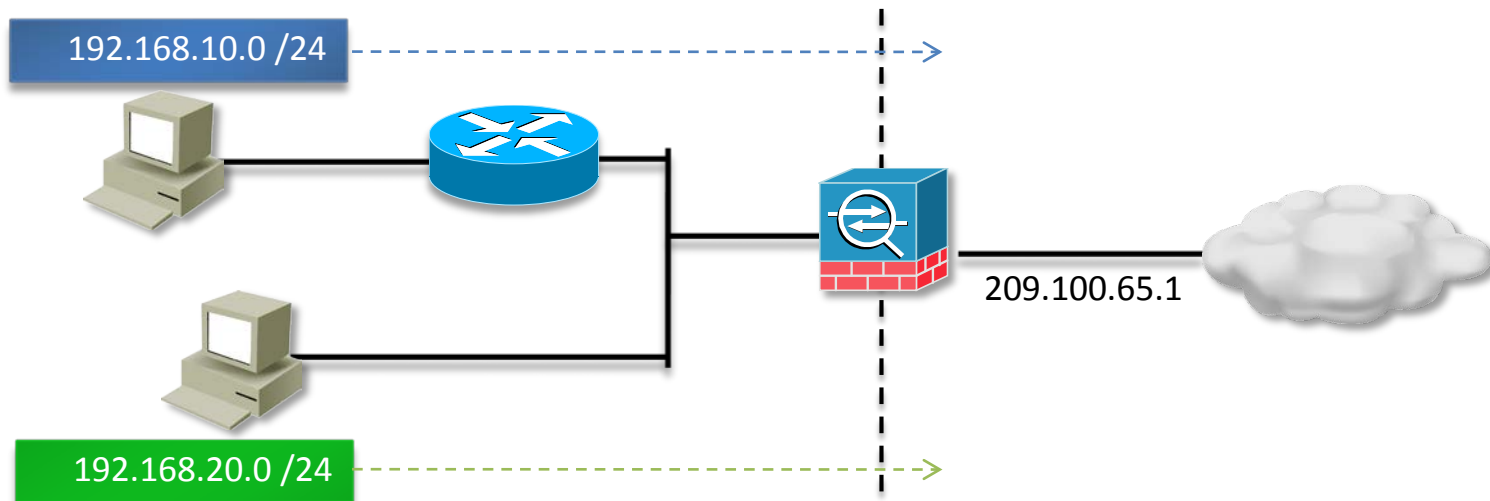
- ▶ Traduce **X** adrese private în **X** adrese publice
- ▶ Una din soluțiile posibile pentru un scenariu în care traficul nu conține porturi la nivelul 4 (GRE, Reliable Datagram Protocol, Data Delivery Protocol, etc)



```
Waters(config)# nat (inside) 1 192.168.10.0 255.255.255.0
Waters(config)# global (outside) 1 209.100.65.2-209.100.65.254
netmask 255.255.255.0
```

- ▶ Comanda nat definește interfața de ingress pentru traficul ce trebuie tradus alături de rețeaua ce va fi tradusă
- ▶ Comanda global definește interfața de egress pentru traficul ce trebuie tradus alături de pool-ul de adrese publice în care se va face traducerea

# Dynamic NAT – două rețele

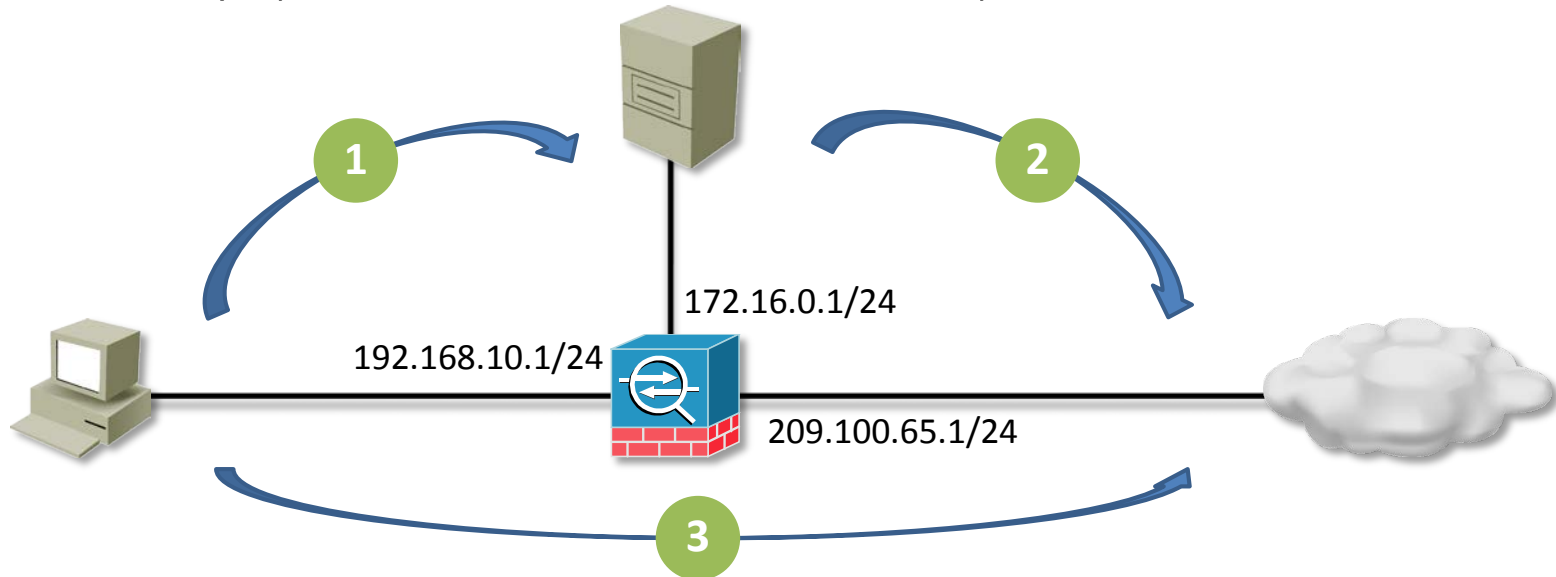


```
Waters(config)# nat (inside) 1 192.168.10.0 255.255.255.0
Waters(config)# nat (inside) 2 192.168.20.0 255.255.255.0
Waters(config)# global (outside) 1 209.100.65.2-209.100.65.120
netmask 255.255.255.0
Waters(config)# global (outside) 2 209.100.65.121-209.100.65.254
netmask 255.255.255.0
```

- Identificatorul din **nat** și **global** este folosit pentru a face legătura dintre cele două comenzi

# Dynamic NAT – noțiuni avansate

- Pentru fiecare conexiune ce face match pe o comandă **nat**, trebuie să existe cel puțin o comandă **global** cu același **ID**

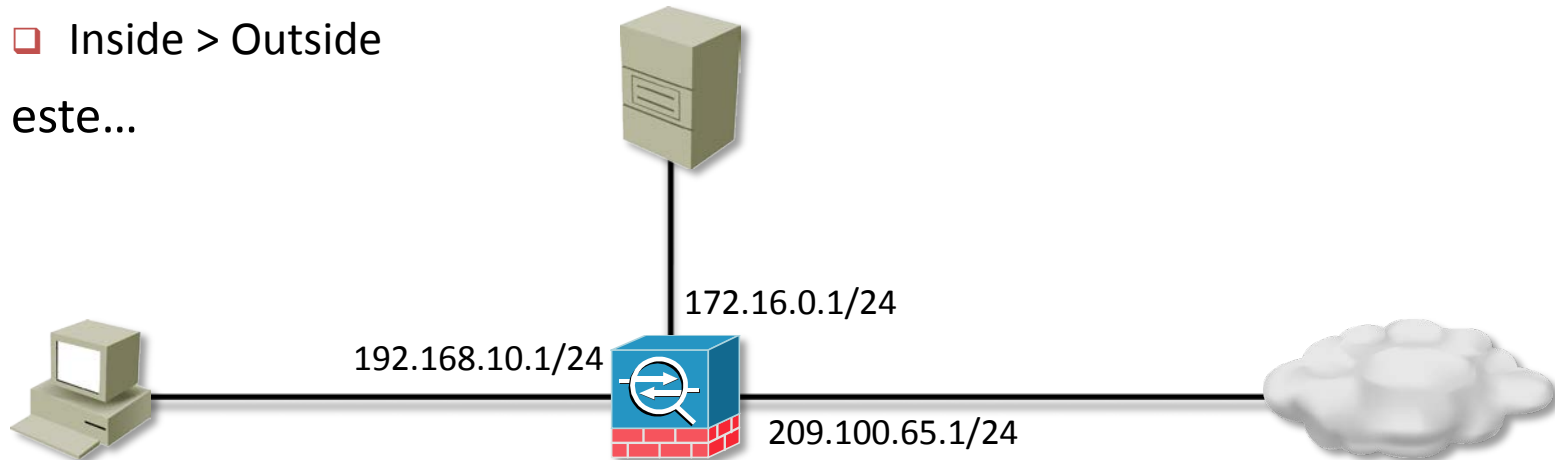


```
Waters(config)# nat (inside) 1 192.168.10.0 255.255.255.0
Waters(config)# nat (dmz) 1 172.16.0.0 255.255.255.0
Waters(config)# global (outside) 1 209.100.65.2-209.100.65.254
netmask 255.255.255.0
```

- În topologia de mai sus nu funcționează comunicare între 2 dintre cele 3 rețele din cauza configurației NAT. **Care este aceasta?**

# Dynamic NAT – problem solved

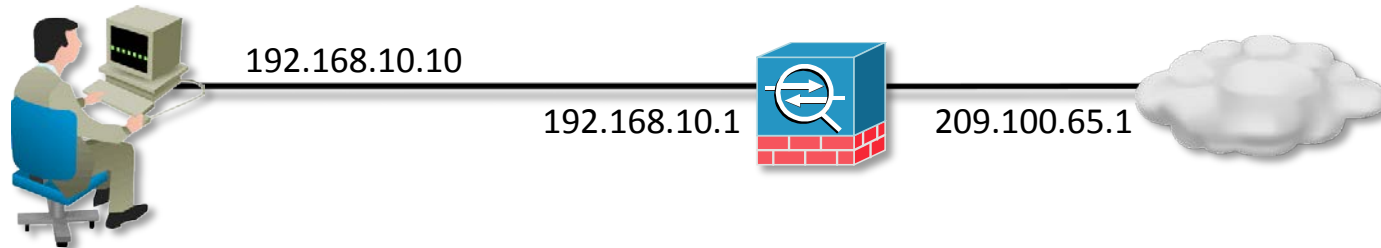
- Configurația corectă pentru a oferi accesul
  - ❑ Inside > DMZ
  - ❑ DMZ > Outside
  - ❑ Inside > Outside
- este...



```
Waters(config)# nat (inside) 1 192.168.10.0 255.255.255.0
Waters(config)# nat (dmz) 1 172.16.0.0 255.255.255.0
Waters(config)# global (outside) 1 209.100.65.2-209.100.65.254
netmask 255.255.255.0
Waters(config)# global (dmz) 1 172.16.0.120-172.16.0.254
netmask 255.255.255.0
```

# Port address translation

- Folosit pentru a translata mai multe adrese private într-o singură adresă publică



```
Waters(config)# nat (inside) 1 192.168.10.0 255.255.255.0
Waters(config)# global (outside) 1 209.100.65.2 netmask
255.255.255.255
```

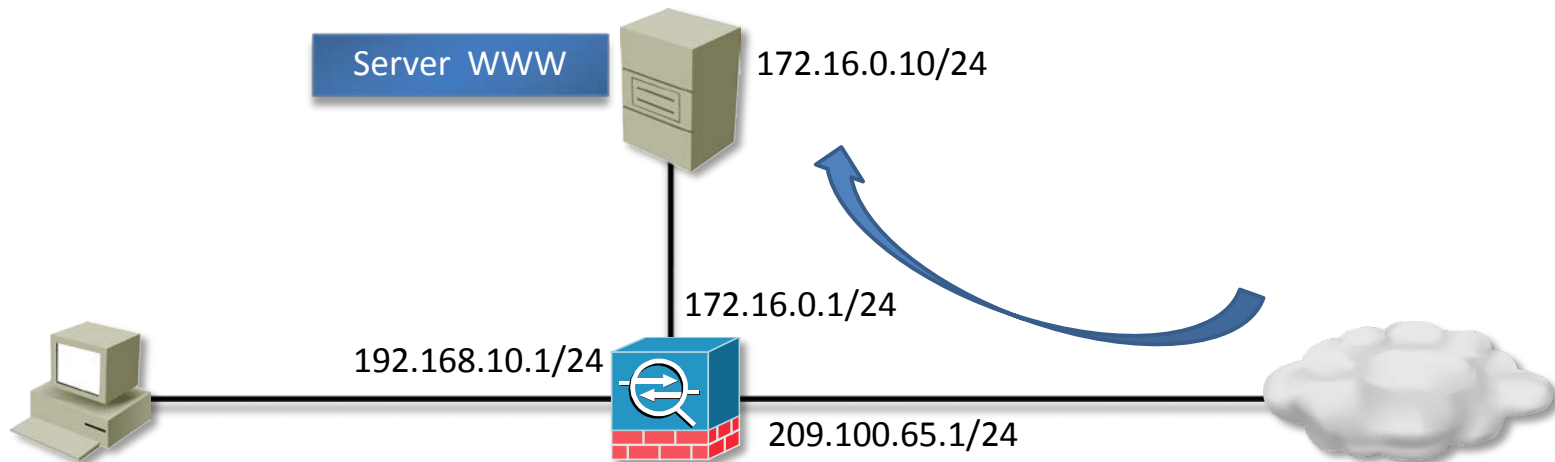
sau

```
Waters(config)# nat (inside) 1 192.168.10.0 255.255.255.0
Waters(config)# global (outside) 1 interface
```



# Static PAT

- ▶ Este de fapt port forwarding/port redirection
- ▶ Se aplică pentru traficul care vine de la o interfață cu nivel de securitate mic la o interfață cu nivel de securitate mare

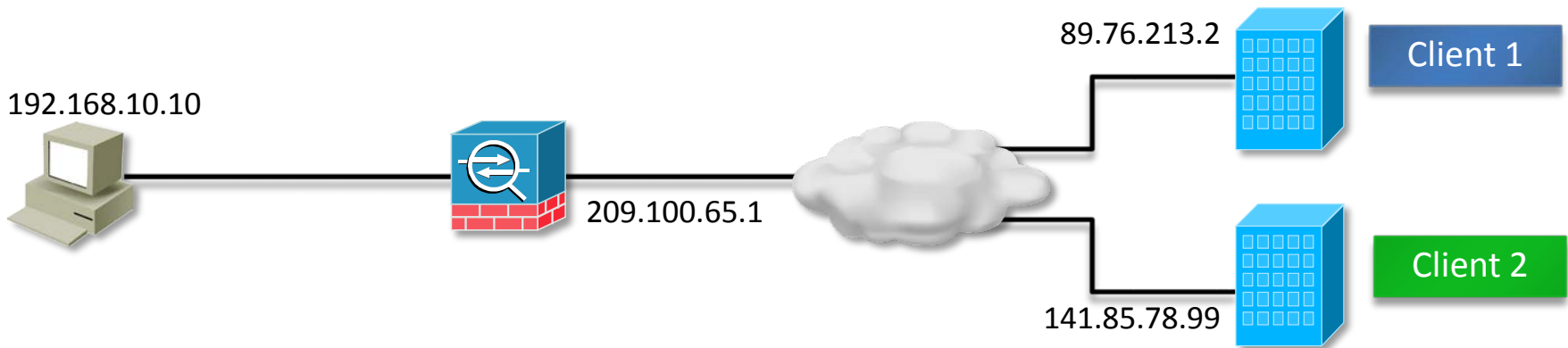


```
Waters(config)# static (dmz,outside) tcp 209.100.65.1 www  
172.16.0.10 www netmask 255.255.255.255
```

- ▶ Redirecțarea se poate face către orice port al oricărei stații din rețeaua internă/DMZ

# Policy NAT/PAT

- Funcție de sursă și destinație se pot aplica translații diferite



```
Waters(config)# access-list policy_PAT1 permit ip host
192.168.10.10 host 89.76.213.2
Waters(config)# access-list policy_PAT2 permit ip host
192.168.10.10 host 141.85.78.99
Waters(config)# nat (inside) 1 access-list policy_PAT1
Waters(config)# nat (inside) 2 access-list policy_PAT2
Waters(config)# global (outside) 1 209.165.100.226
Waters(config)# global (outside) 2 209.165.100.227
```

# Nat-Control

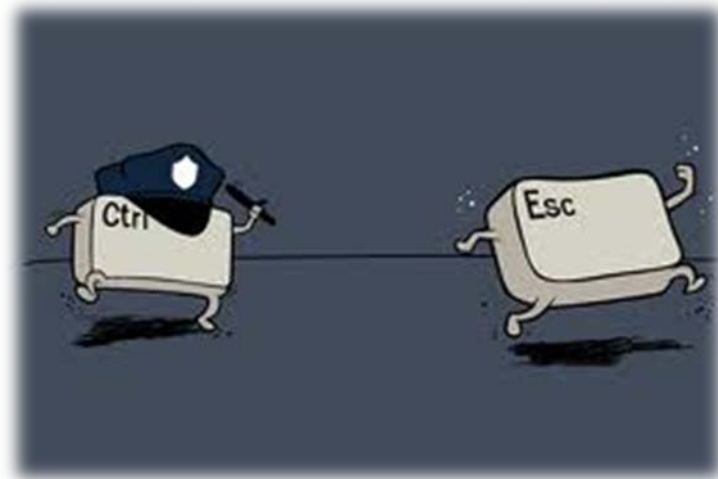
---

- ▶ Comanda **nat-control** specifică blocarea explicită de către ASA a traficului ce nu este identificat prin nici o comanda **nat**
- ▶ Înainte de versiunea 7.x era *enabled* în mod implicit
- ▶ Explicație 1: o funcționalitate de securitate care pleacă de la ideea că orice trafic ce încearcă să iasă din rețea ocolind regulile de NAT ale administratorului (spoof) trebuie blocat
- ▶ Explicație 2: o funcționalitate de securitate care ajută blocarea traficului pentru care administratorul a omis să configureze NAT sau a făcut configurații incorecte

# NAT bypass

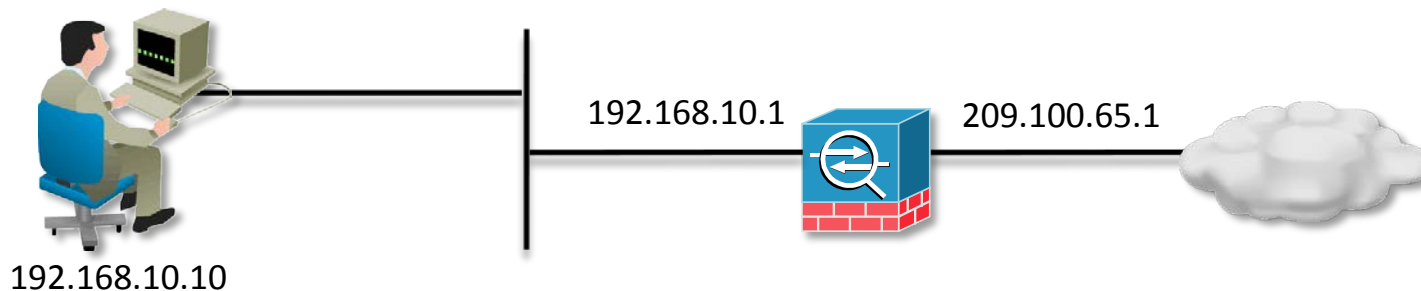
---

- ▶ Când nat-control este activat trebuie să existe o metodă de a putea face o excepție și a trece totuși trafic fără a aplica NAT
- ▶ Chiar și fără nat-control există situații când dorim bypass la NAT pentru anumite comunicații
- ▶ Există două metode:
  - ❑ Identity NAT
  - ❑ NAT Exemption



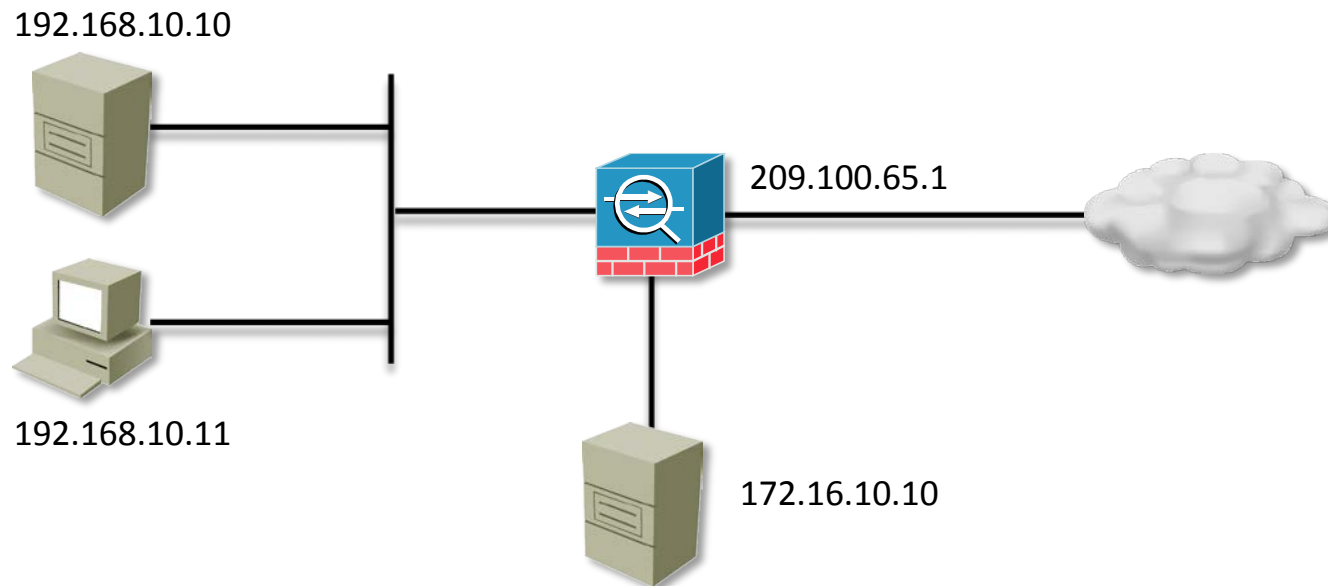
# Identity NAT

- Identity NAT se configurează folosind identificatorul special “0”



```
Waters(config)# nat-control
Waters(config)# nat (inside) 1 192.168.10.0 255.255.255.0
Waters(config)# global (outside) 1 209.100.65.2-209.100.65.254
netmask 255.255.255.0
Waters(config)# nat (inside) 0 192.168.10.10 255.255.255.255
```

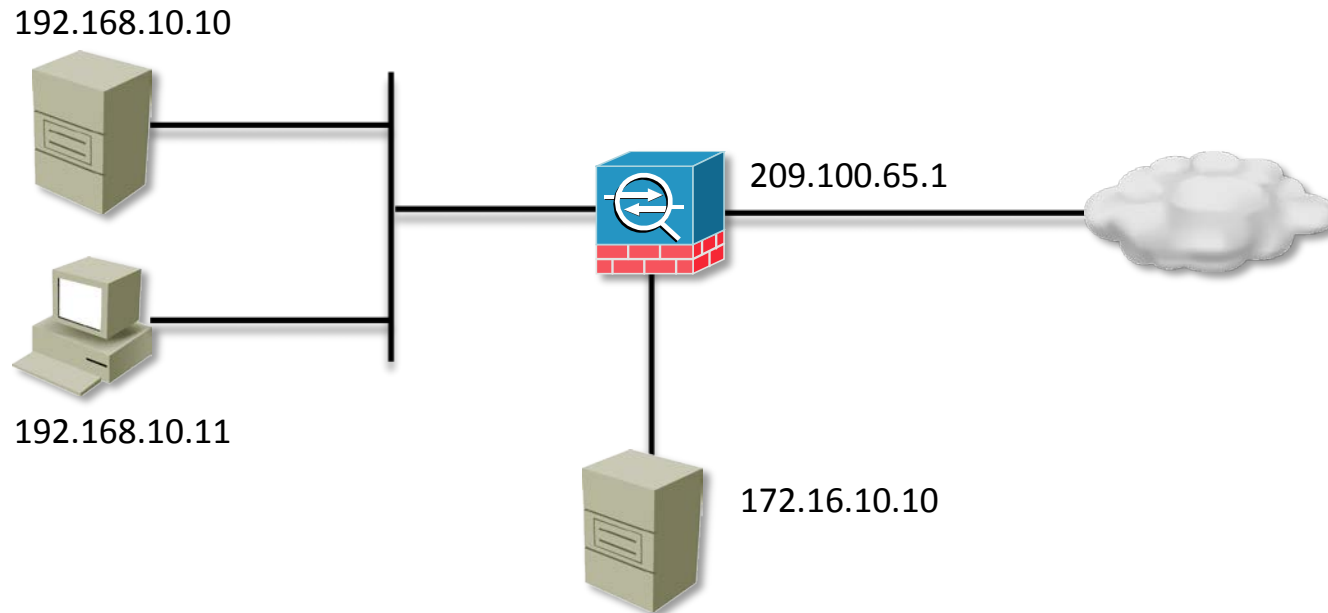
# NAT Exemption



## ► Scenariu:

- ❑ Administratorul are adresare privată atât în LAN cât și în DMZ
- ❑ Administratorul dorește să ofere acces la NET din LAN și DMZ
- ❑ Administratorul are un server de mail în LAN și unul public în DMZ
- ❑ Administratorul nu dorește ca traficul între cele 2 servere să fie trecut prin NAT indiferent de serverul care inițiază comunicarea

# NAT Exemption

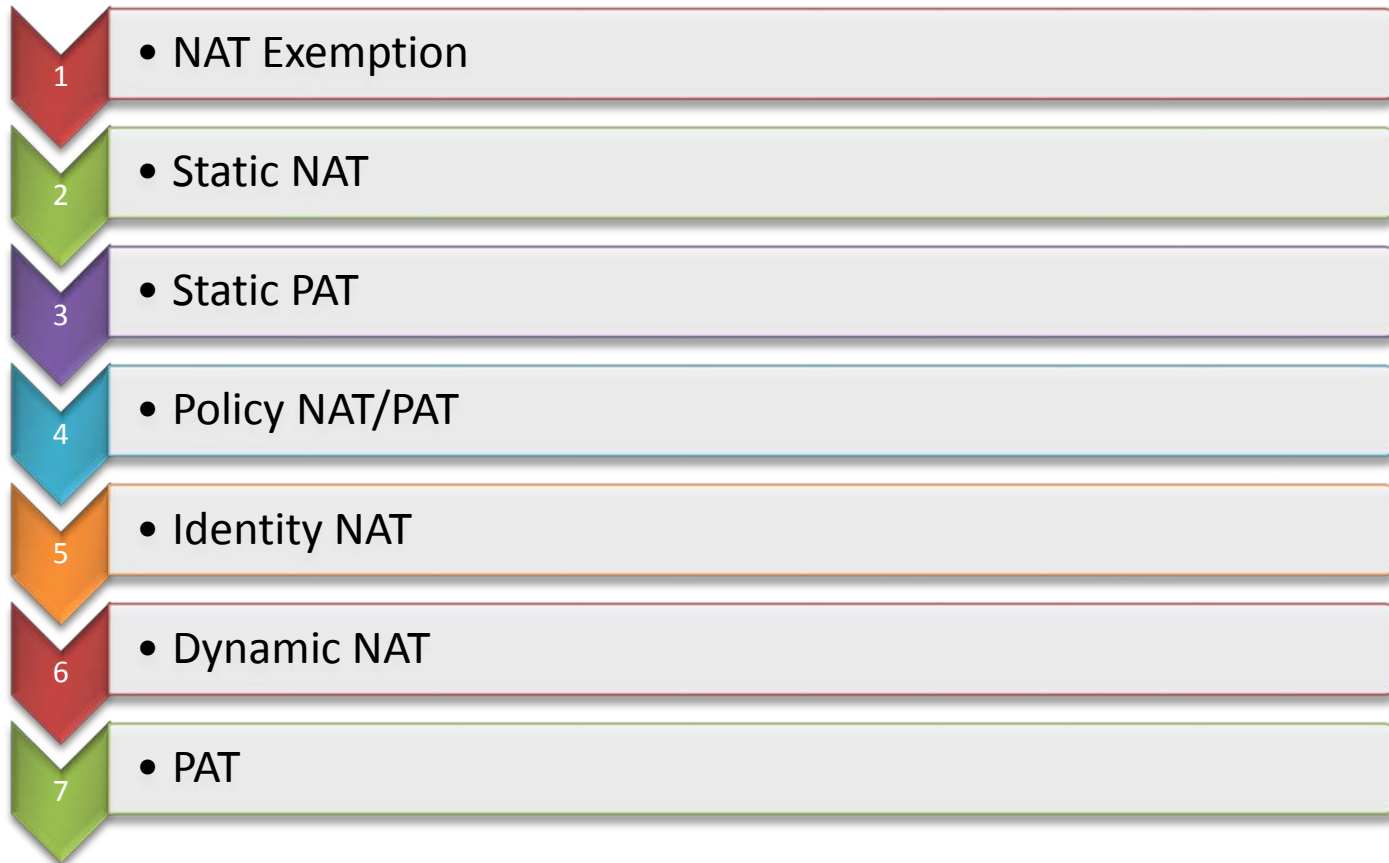


```
Waters(config)# access-list Email_Servers extended permit ip  
host 192.168.10.10 host 172.16.10.10  
Waters(config)# nat (inside) 0 access-list Email_Servers  
Waters(config)# nat (inside) 1 192.168.10.0 255.255.255.0  
Waters(config)# nat (dmz) 1 172.16.10.0 255.255.255.0  
Waters(config)# global (outside) 1 interface
```

# Ordinea operațiilor NAT

---

- ▶ La procesarea NAT, firewall-ul ASA aplică următoarele priorități





# Verificarea tabelii de translații

---

- Tabela este numită “xlate” în ASA OS

```
Waters#show xlate
1 in use, 2 most used
Global 209.100.65.1 Local 192.168.10.10
```

- Mai multe informații prin cuvântul cheie “detail”

```
Waters# show xlate detail
1 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - dynamic, n - no random, r -
      portmap, s - static
NAT from inside:192.168.10.10 to outside:209.100.65.1 flags i
```

# Verificarea tabelii de translații

---

```
Waters# show local-host
```

```
Interface inside: 1 active, 1 maximum active, 0 denied
```

```
local host: <192.168.10.10>,
```

```
    TCP flow count/limit = 1/unlimited
```

```
    TCP embryonic count to (from) host = 0 (0)
```

```
    TCP intercept watermark = unlimited
```

```
    UDP flow count/limit = 0/unlimited
```

```
Xlate:
```

```
    PAT Global 209.165.200.225(1024) Local 192.168.10.10(11085)
```

```
Conn:
```

```
    TCP out 209.165.200.240:23 in 192.168.10.10:11085 idle 0:00:13 bytes  
    87 flags UIO
```

- Comanda arată atât conexiuni cât și translatări, atât cele de management cât și cele rutate



## Lucrul avansat cu ACL-uri

# ACL refresher

---

## ► Definirea unui ACL

```
Waters(config)#access-list exemplu line 1 extended deny tcp 192.168.1.0  
255.255.255.0 any eq 80  
Waters(config)#access-list exemplu line 2 extended deny tcp 192.168.1.0  
255.255.255.0 any eq 25  
Waters(config)# access-list exemplu line 10 extended permit ip any any
```

## ► Aplicarea unui ACL pentru filtrare

```
Waters(config)# access-group exemplu in interface outside
```


## ► Afişarea unui ACL

```
Waters(config)# sh access-list
```

# Editarea unui ACL

- ▶ Se dă următorul ACL

```
Waters(config)# sh access-1
access-list exemplu; 5 elements
access-list exemplu line 1 extended deny tcp 192.168.1.0
255.255.255.0 any eq www (hitcnt=0) 0xeb5a9c13
access-list exemplu line 2 extended deny tcp 192.168.1.0
255.255.255.0 any eq smtp (hitcnt=0) 0xc8a35917
access-list exemplu line 3 extended deny udp any any (hitcnt=0)
0x9697394d
access-list exemplu line 4 extended deny icmp any any echo
(hitcnt=0) 0x4992c99e
access-list exemplu line 5 extended permit ip any any
(hitcnt=0) 0x51092e5b
```



- ▶ Se dorește adăugarea unei intrări între linia 2 și 3

# Editarea unui ACL

---

- La introducerea unei linii ce deja există, se face shiftare în ACL

```
Waters(config)# access-list exemplu line 3 extended permit udp
any any eq 520
Waters(config)# sh access-1
access-list exemplu; 6 elements
access-list exemplu line 1 extended deny tcp 192.168.1.0
255.255.255.0 any eq www (hitcnt=0) 0xeb5a9c13
access-list exemplu line 2 extended deny tcp 192.168.1.0
255.255.255.0 any eq smtp (hitcnt=0) 0xc8a35917
access-list exemplu line 3 extended permit udp any any eq rip
(hitcnt=0) 0x48551218
access-list exemplu line 4 extended deny udp any any (hitcnt=0)
0x9697394d
access-list exemplu line 5 extended deny icmp any any echo
(hitcnt=0) 0x4992c99e
access-list exemplu line 6 extended permit ip any any
(hitcnt=0) 0x51092e5b
```

# Comentarea unui ACL

---

```
Waters(config)# access-list exemplu line 3 remark Linia
urmatoare permite RIP
Waters(config)# sh access-l
access-list exemplu; 6 elements
access-list exemplu line 1 extended deny tcp 192.168.1.0
255.255.255.0 any eq www (hitcnt=0) 0xeb5a9c13
access-list exemplu line 2 extended deny tcp 192.168.1.0
255.255.255.0 any eq smtp (hitcnt=0) 0xc8a35917
access-list exemplu line 3 remark Linia urmatoare permite RIP
access-list exemplu line 4 extended permit udp any any eq rip
(hitcnt=0) 0x48551218
access-list exemplu line 5 extended deny udp any any (hitcnt=0)
0x9697394d
access-list exemplu line 6 extended deny icmp any any echo
(hitcnt=0) 0x4992c99e
access-list exemplu line 7 extended permit ip any any
(hitcnt=0) 0x51092e5b
```

# Ștergerea unui ACL

---

- ▶ Se poate șterge o singură linie de oriunde din ACL

```
Waters(config)# no access-list exemplu line 5 extended deny udp  
any any
```

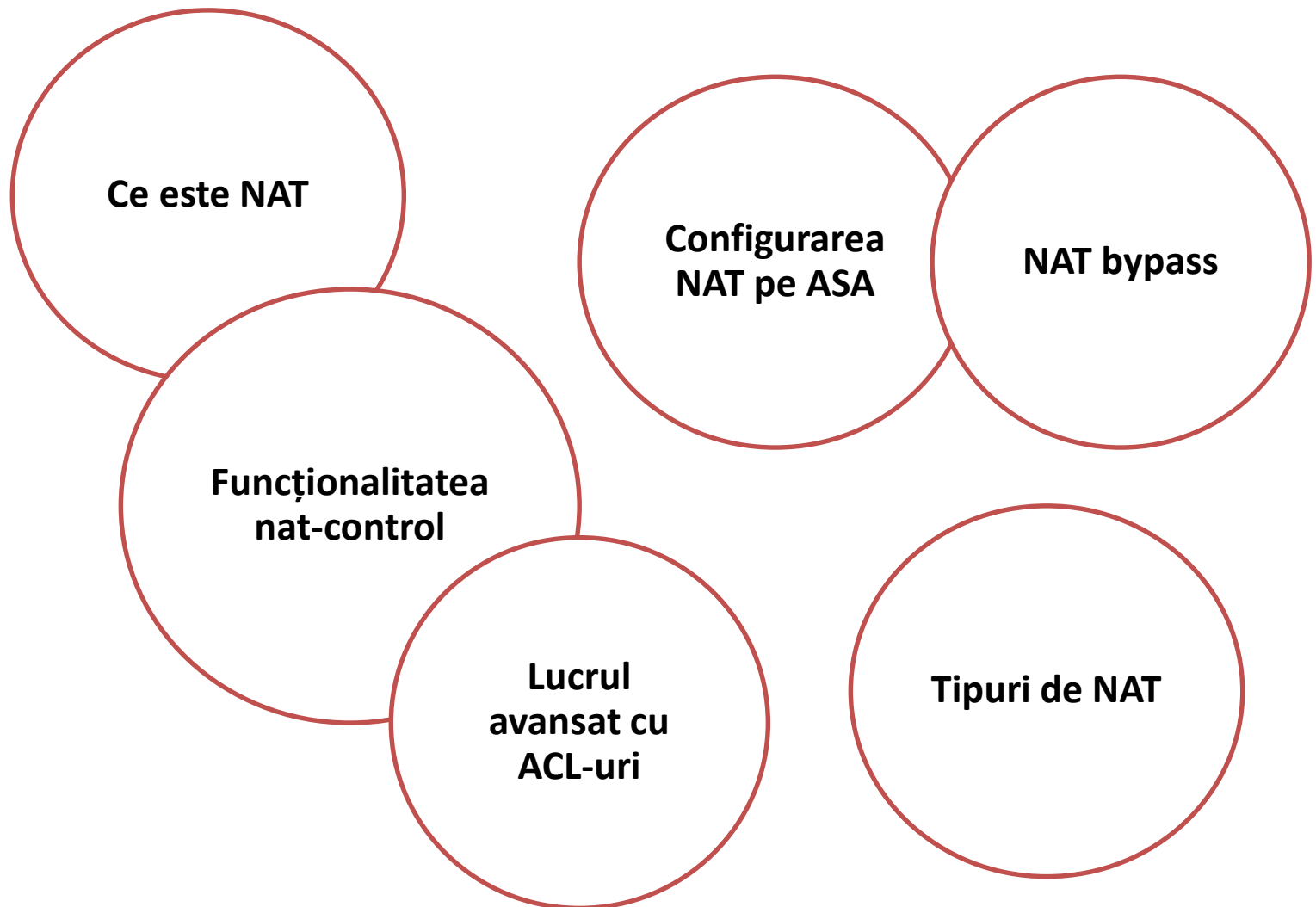
- ▶ Sau întregul ACL

```
Waters(config)# clear configure access-list exemplu  
Waters(config)# sh access-l  
access-list cached ACL log flows: total 0, denied 0 (deny-flow-  
max 4096)  
alert-interval 300
```



# Overview

---



# Cursul viitor...

---

## ► Application Inspection

- ❑ Studiu de caz: Active FTP/Passive FTP
- ❑ Putem permite un protocol fără a îl inspecta?
- ❑ Ce se întâmplă dacă HTTP nu mai rulează pe portul 80?
- ❑ Configurarea parametrilor DNS/SMTP

## ► ACL Object grouping

