КАК – CISCO ASA 5505 nat global static

В общем так. Стало с одной стороны проще, с другой сложнее. Они убрали зоопарк команд **nat**, **global** и **static** и теперь есть только команда **nat**. Но зато есть 2 варианта. Они их называют **Network Object NAT** и **Twice NAT**. Первый чуть сложнее, но привычнее. Второй новый и проще. Начну со второго.

Гравное отличие от старого доброго static – нельзя прямо в самой команде ната указывать ip-адреса. Сначала нужно командами **object network** описать что и во что натить, а потом командой **nat** связать всё это в кучу Например так:

```
hostname(config)# object network FTP_ SERVER_PUBLIC
hostname(config-service-object)# host 100.100.100.100
hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100
hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface FTP_
SERVER_PUBLIC
```

Обрати внимание, что команда **nat** даётся просто из режима конфигурации, не из режима конфигурации объекта, т.е. это просто отдельная команда, не связанная с режимом конфигурации объекта, в отличии от Twice NAT. Понятно, что эту команду можно давать и не выходя из конфигурации объекта, она сама дальше напишет `hostname(config)#`, но тут суть именно в том, что это просто отдельная команда и будет в текстовом конфиге ниже по тексту, там где привыкли видеть статики и наты с глобалами.
Вместо слова **static** можно написать **dynamic**. Тогда можно в первом и втором объекте указывать не только хост, но и сеть. Если при этом вторая сеть будет меньше первой, то сначала будет NAT, а с последним адресом PAT/ Но тут ничего нового, раньше было также.
Вместо второго объекта можно написать **interface**, если нужно натить в адрес интерфейса, указанного вторым в скобках после самой команды **nat** (в нашем примере **outside**).

Главные отличия этого метода, ключевое слово **source**, команда **nat** отдельно от объявления объекта(ов) **object network** и указание и того, что натить и того, во что натить в одной команде.

Network Object NAT характерен тем, что команда **nat** присутствует прямо в разделе **object network**. Кроме того, нет слова **source** и в качестве того, во что натить можно использовать не **object network**, а просто адрес или сетку. Предыдущий пример тогда будет выглядеть так:

```
hostname(config)# object network FTP_ SERVER_PUBLIC
hostname(config-service-object)# host 100.100.100.100
hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100
hostname(config-network-object)# nat (inside,outside) static FTP_ SERVER_PUBLIC
```

или так:

```
hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100
hostname(config-network-object)# nat (inside,outside) static 100.100.100.100
```

Аналогично можно использовать **dynamic** вместо **static**.
В самом текстовом конфиге будет интересно. В верхней части будет объявление объектов с указанием хостов/сетей, а ниже, там где всё про нат, будет ещё раз типа объявления объекта, но уже без хоста/сети, а только с командой **nat**. Вот кусок моего боевого конфига для примера, **Twice NAT** нет, только **Network Object NAT:**

```
interface Ethernet0/0
nameif outside
security-level 0
ip address 10.4.100.251 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 172.20.10.230 255.255.255.0
```

```
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
nameif management
security-level 0
ip address 10.4.1.245 255.255.255.0
!
boot system disk0:/asa913-k8.bin
ftp mode passive
clock timezone AMST 4
clock summer-time AMDT recurring last Sun Mar 2:00 last Sun Oct 3:00
dns domain-lookup outside
dns server-group DefaultDNS
name-server 10.4.100.11
name-server 10.4.100.10
domain-name cpcpipe.ru
object network NET_M42PHN38
host 172.20.10.3
object network NET_M42PHN39
host 172.20.10.2
access-list INSIDE_ACCESS_IN extended permit icmp object NET_M42PHN38 10.4.0.0 255.255.0.0
access-list INSIDE_ACCESS_IN extended permit tcp object NET_M42PHN38 host 10.4.100.30 eq smtp
access-list INSIDE_ACCESS_IN extended permit icmp object NET_M42PHN39 10.4.0.0 255.255.0.0
access-list INSIDE_ACCESS_IN extended permit tcp object NET_M42PHN39 host 10.4.100.30 eq smtp
access-list INSIDE_ACCESS_IN extended permit udp object NET_M42PHN39 host 10.4.1.233 eq snmp
access-list INSIDE_ACCESS_IN extended permit udp object NET_M42PHN39 host 10.4.42.126 eq ntp
access-list OUTSIDE_ACCESS_IN extended permit icmp 10.4.0.0 255.255.0.0 object NET_M42PHN38
access-list OUTSIDE_ACCESS_IN extended permit tcp 10.4.0.0 255.255.0.0 object NET_M42PHN38 eq www
access-list OUTSIDE_ACCESS_IN extended permit tcp 10.4.0.0 255.255.0.0 object NET_M42PHN38 eq 3389
access-list OUTSIDE_ACCESS_IN extended permit tcp 10.4.0.0 255.255.0.0 object NET_M42PHN38 eq 4899
access-list OUTSIDE_ACCESS_IN extended permit icmp 10.4.0.0 255.255.0.0 object NET_M42PHN39
access-list OUTSIDE_ACCESS_IN extended permit tcp 10.4.0.0 255.255.0.0 object NET_M42PHN39 eq www
access-list OUTSIDE_ACCESS_IN extended permit tcp 10.4.0.0 255.255.0.0 object NET_M42PHN39 eq https
pager lines 24
logging enable
logging buffer-size 10000
logging console errors
logging buffered errors
logging trap warnings
logging host outside 10.4.1.24
mtu inside 1500
mtu management 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-714.bin
no asdm history enable
```

```
arp timeout 14400
no arp permit-nonconnected
!
object network NET_M42PHN38
nat (inside,outside) static 10.4.100.238
object network NET_M42PHN39
nat (any,any) static 10.4.100.239
access-group INSIDE_ACCESS_IN in interface inside
access-group OUTSIDE_ACCESS_IN in interface outside
route outside 10.4.0.0 255.255.0.0 10.4.100.254 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
```