Cisco NAT Cheat Sheet

Version 1.0

Order of Operations

ASA Pre-8.3

- -NAT exemption (nat 0) (in order of configuration)
- -Existing flows (established translations)
- -Static NAT and Static PAT (regular and policy) (in order of configuration)
- -Dynamic Policy NAT (in order of configuration)
- -Regular Dynamic NAT (best match)

ASA Post-8.3

- -Existing Flows
- -Manual NAT (AKA: Policy NAT, Twice NAT, Identity NAT) (Static and Dynamic) (in order of configuration)
- -Static Object NAT (Auto-NAT) w/ Single Real IP
- -Static Object NAT w/ Multiple Real IP
- -Dynamic Object NAT w/ Single Real IP
- -Dynamic Object NAT w/ Multiple Real IP
- -Manual NAT (AKA: Policy NAT, Twice NAT, Identity NAT) w/ 'After-Auto' option (Static and Dynamic)

Useful Links and References

More ASA Pre-8.3 to 8.3 Configuration Cxamples

ASA 8.3+ NAT Order of Operations

ASA 8.2 NAT Order of Operations

Regular Static NAT (One IP to One Server)

ASA Pre-8.3

```
static (inside,outside) 2.0.0.1 10.1.1.6 netmask  255.255.255.255
```

ASA Post-8.3

```
object network obj-10.1.1.6
  host 10.1.1.6
  nat (inside,outside) static 2.0.0.1
```

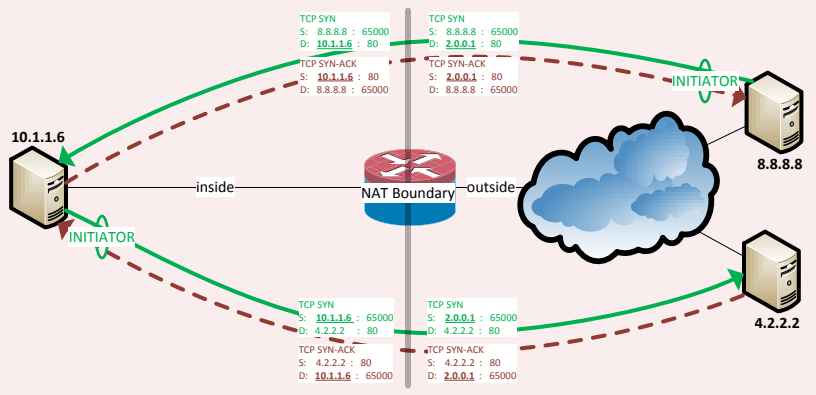
IOS

```
interface FastEthernet0/0
 ip nat outside
!
interface FastEthernet0/1
 ip nat inside
!
ip nat inside source static 10.1.1.6 2.0.0.1
```

Notes:
This type of NAT is most commonly used for presenting an internally hosted service (WWW, SMTP, etc) to the public internet.

Since all ports are passed through this type of NAT, you should use an externally facing access-list to permit only certain ports through to the inside

It allows flows to be initiated from either side and masks the private IP of the internal service



Regular Static PAT (One IP to Multiple Servers)

ASA Pre-8.3

```
static (inside,outside) tcp 2.0.0.1 8080 10.1.1.6 80 netmask  255.255.255.255
```

ASA Post-8.3

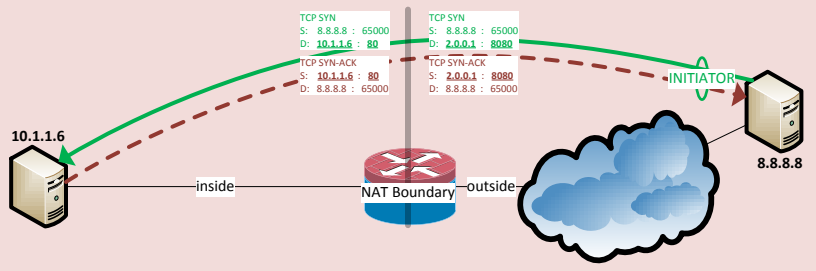
```
object network obj-10.1.1.6
  host 10.1.1.6
  nat (inside,outside) static 2.0.0.1 service tcp www 8080
```

IOS

```
interface FastEthernet0/0
 ip nat outside
!
interface FastEthernet0/1
 ip nat inside
!
ip nat inside source static tcp 10.1.1.6 80 2.0.0.1 8080 extendable
```

Notes:
This type of NAT is most commonly used for making services on multiple internal hosts available to the internet using the same public IP (usually used when public IP space is tight). ie: RTR1 Telnet available on 2.0.0.1:2323, RTR2 Telnet available on 2.0.0.1:2324, etc.

It only allows flows to be initiated from one side (the outside), as it is performing PAT on the destination port and IP (from the perspective of the SYN). To initiate traffic from the inside, and still tick this NAT rule, you would have to control your source port (which is atypical).



Static Policy NAT

ASA Pre-8.3

```
access-list NET1 permit ip host 10.1.1.6 8.0.0.0 255.0.0.0
!
static (inside,outside) 2.0.0.1 access-list NET1
```

ASA Post-8.3

```
object network obj-10.1.1.6
  host 10.1.1.6
!
object network obj-2.0.0.1
  host 2.0.0.1
!
object network obj-8.0.0.0
  subnet 8.0.0.0 255.0.0.0
!
nat (inside,outside) source static obj-10.1.1.6 obj-2.0.0.1 destination static obj-8.0.0.0 obj-8.0.0.0
```

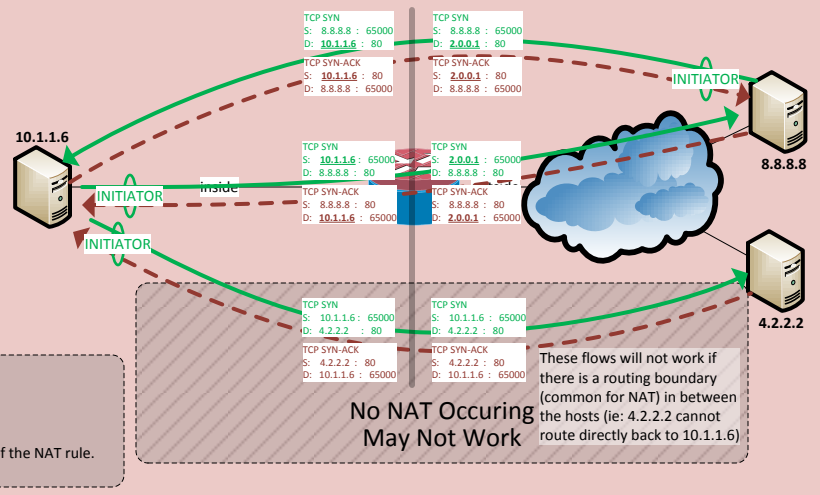
IOS

```
interface FastEthernet0/0
 ip nat outside
!
interface FastEthernet0/1
 ip nat inside
!
ip access-list extended NAT
 permit ip any 8.0.0.0 0.255.255.255
 deny   ip any any
!
route-map NAT permit 10
 match ip address NAT
!
ip nat inside source static 10.1.1.6 2.0.0.1 route-map NAT
```

Notes:
Policy NAT is commonly used to create more specific match criteria for a NAT rule (ie: Destination IP , Source Port, etc).

The access-list (in IOS and pre-8.3) is only used for matching initiating traffic, it is not used for the translation itself. The 8.3 version does not use an access-list.

It allows flows to be initiated by either side. When originating the flow from the outside, you must use a source IP that is covered by the destination element of the NAT rule. When originating from the inside, you must ensure that the destination IP is covered by the destination element of the NAT rule.



Regular Dynamic Interface NAT/PAT (Basic Internet Access)

ASA Pre-8.3

```
global (outside) 1 interface
!
nat (inside) 1 0.0.0.0 0.0.0.0
```

ASA Post-8.3

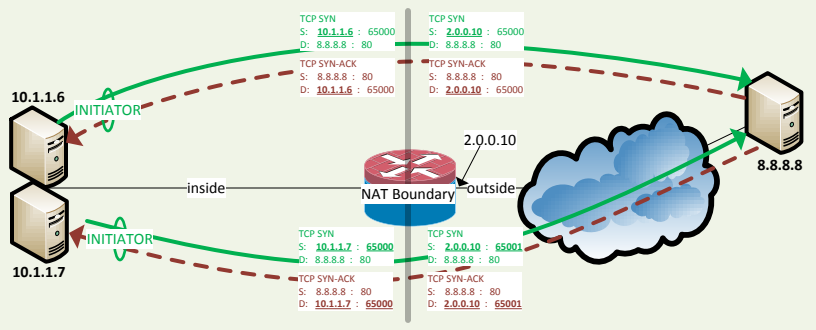
```
object network ANY
  subnet 0.0.0.0 0.0.0.0
   nat (inside,outside) dynamic interface
```

IOS

```
interface FastEthernet0/0
 ip nat outside
!
interface FastEthernet0/1
 ip nat inside
!
access-list 10 permit any
!
ip nat inside source list 10 interface FastEthernet0/0 overload
```

Notes:
This type of NAT is commonly used to provide internet access for a group of internet hosts via a fixed public IP, which is the same public IP as is held by the NAT device interface

It only allows flows to be initiated from one side (the inside), as it is performing NAT and/or PAT on the source address of the initiator (from the perspective of the SYN).



Regular Dynamic NAT/PAT (Basic Internet Access)

ASA Pre-8.3

```
global (outside) 1 2.0.0.1
!
nat (inside) 1 0.0.0.0 0.0.0.0
```

ASA Post-8.3

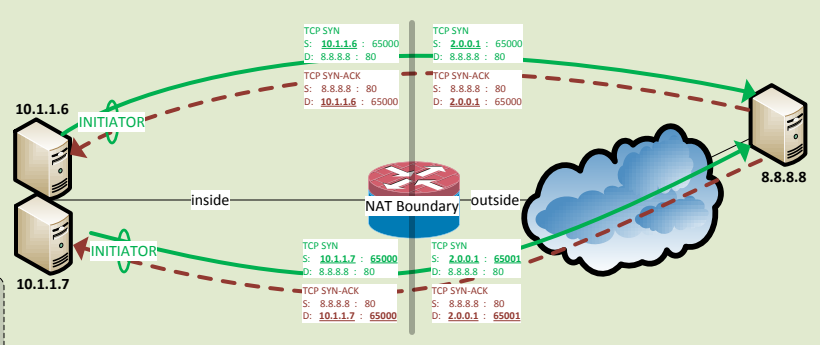
```
object network ANY
  subnet 0.0.0.0 0.0.0.0
   nat (inside,outside) dynamic 2.0.0.1
```

IOS

```
interface FastEthernet0/0
 ip nat outside
!
interface FastEthernet0/1
 ip nat inside
!
ip nat pool NATPOOL 2.0.0.1 2.0.0.1 netmask 255.255.255.252
!
access-list 10 permit any
!
ip nat inside source list 10 pool NATPOOL overload
```

Notes:
This type of NAT is commonly used to provide internet access for a group of internet hosts via a fixed public IP, without using the public IP of the NAT device.

It only allows flows to be initiated from one side (the inside), as it is performing NAT on the source address of the initiator (from the perspective of the SYN).



Identity NAT/NAT Exemption/No-NAT (With Interface PAT)

ASA Pre-8.3

```
access-list no_nat extended permit ip any 8.0.0.0 255.0.0.0
!
global (outside) 1 interface
!
nat (inside) 0 access-list no_nat
!
nat (inside) 1 0.0.0.0 0.0.0.0
```

ASA Post-8.3

```
object-group network NONAT_LOCAL
 network-object 10.0.0.0 255.0.0.0
 !
object-group network NONAT_REMOTE
 network-object 8.0.0.0 255.0.0.0
 !
nat (inside,outside) source static NONAT_LOCAL NONAT_LOCAL destination static NONAT_REMOTE NONAT_REMOTE route-lookup
```

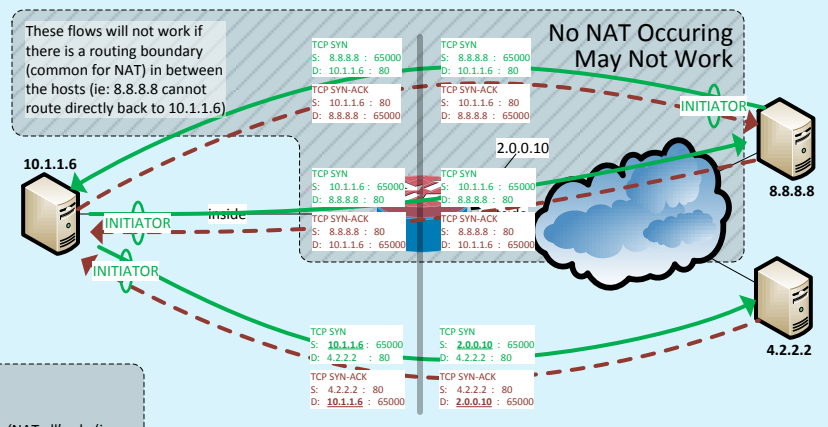
IOS

```
interface FastEthernet0/0
 ip nat outside
!
interface FastEthernet0/1
 ip nat inside
!
ip access-list extended NONAT
 deny   ip 10.0.0.0 0.255.255.255 8.0.0.0 0.255.255.255
 permit ip any any
!
route-map NAT permit 10
 match ip address NAT
!
ip nat inside source route-map NAT interface FastEthernet0/0 overload
```

Notes:
Identity NAT is a form of policy NAT which matches specific flows and 'NATs them to themselves', meaning that it doesn't change any of the addressing.

Identity NAT is usually used in places where you have a NAT boundary which translates all traffic passing through (ie: internet firewall). It is entered above the 'NAT all' rule (in the order of operations) to effectively negate the 'NAT all' for the specified flows. It is typically useful when you have some kind of VPN terminating to a device that is otherwise a 'NAT all' device.

It allows flows to be initiated from either side, as long as the source and destination addresses are properly specified in the rule



Created by John W Kerns

blog.packetsar.com