

FORMAÇÃO EM CIBERSEGURANÇA

CISCO SECURE FIREWALL - NAT

CIBERSEGURANCA.CISCO.COM.BR

JANEIRO/2025

DISCLAIMER

Esse material não tem qualquer relação oficial com a empresa CISCO. Ele foi criado por um profissional que trabalha há 20 anos com os equipamentos e soluções do fabricante.

A configuração mostrada não é uma recomendação. O autor não se responsabiliza por má utilização do material, que tem objetivo exclusivamente educativo (use-o para testar e aprender a ferramenta).

Esse ebook foi constituído a partir de artigos publicados de 2019 a 2021 no blog da TechRebels no medium.com pelo mesmo autor.


PARTE 1

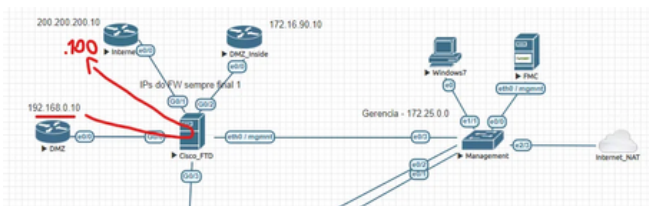
Até a versão **8.2 do ASA**, havia somente uma versão de NAT disponível – com algumas variações na sua aplicação. À partir da 8.3, a Cisco incluiu uma possibilidade adicional.

O que o ASA tem a ver com o FTD? Bom, o código do ASA faz parte do FTD e o nome dele é LINA. Após o processamento do pacote em camada 3 e 4, ele envia ao motor do SNORT para inspeção profunda. Em um outro artigo, falaremos mais disso.

Mas enfim, o NAT clássico do ASA agora é o Auto NAT e o NAT “novo” se chama Manual NAT.

Começando pelo NAT clássico então, nossa topologia é essa: vamos traduzir da DMZ para a Internet.

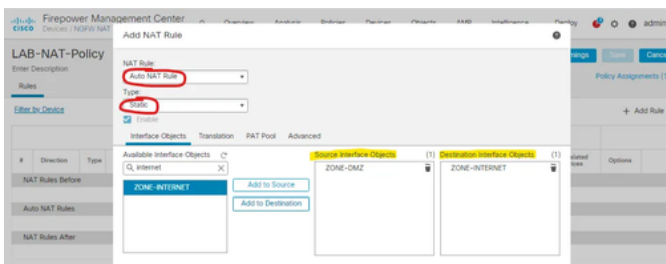
 **Obs:** Os IPs das interfaces do FW são sempre final .1



Imaginando o FW como uma parede, pensamos que o IP 192.168.0.10, ao atravessar a parede, virará um outro IP, no caso o 200.200.200.100.

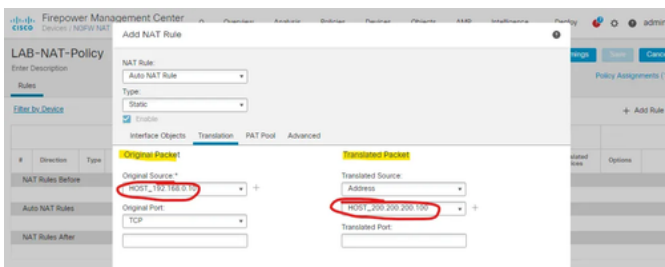
Simples dessa forma. Não importa pra “onde” queremos ir =)

Na imagem abaixo, repare na regra de NAT e no tipo dele em vermelho. Já o amarelo, mostra a interface de origem e a de destino.



Abaixo, repare no pacote original, com o IP 192.168.0.10 e o pacote traduzido 200.200.200.100.





Ao salvar, veja como fica a política de NAT. Em amarelo, significa que vamos traduzir as requisições DNS que derem match nessa regra – essa parte é especificamente importante para o PAT de acesso à internet que veremos adiante.

#	Direction	Type	Original Packet			Translated Packet			Options
			Source Interface	Destination Interface	Original Source	Original Destinations	Original Services	Translated Source	
NAT Rules Before									
*		S...	ZONE-DMZ	ZONE-INTERNET	HOST_192.168.0.1			HOST_200.200.200.100	Yellow
NAT Rules After									

No router de Internet, conseguimos pingar o 200.200.200.100 e ao dar telnet, acessamos o router da DMZ.

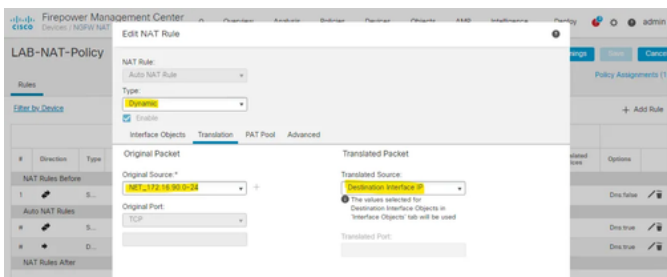
```

Internet
Internet#
Internet#
Internet#
Internet#
Internet#
Internet#
Internet#ping 200.200.200.100 ✓
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.200.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Internet#
Internet#
Internet#telnet 200.200.200.100 ✓
Trying 200.200.200.100 ... Open
User Access Verification
Password: ✓
DMZ:
  
```



Esse tipo de NAT traduz a origem da requisição, e ele é indicado pela Cisco para os casos **simples** de tradução de IP, como por exemplo ao acessarmos a Internet. Da mesma forma poderíamos traduzir uma rede para o IP da interface externa do firewall, fazendo dessa forma um **PAT** — **Port Address Translation** — clássico.

Veja na figura abaixo como ficaria: O tipo de NAT é dinâmico, e a origem é toda a rede da DMZ_Inside. O destino é o IP da interface de destino, no caso, a interface internet.



Ao acessar o router de Internet, à partir do router da DMZ_Inside, veja que a conexão de origem parte do IP 200.200.200.1, que é o IP da interface internet do Firewall.



```

DMZ_Inside#
DMZ_Inside#
DMZ_Inside#
DMZ_Inside#
DMZ_Inside#
DMZ_Inside#
DMZ_Inside#
DMZ_Inside#telnet 200.200.200.10
Trying 200.200.200.10 ... Open

User Access Verification
Password:
Internet>who
      Line          User             Host(s)          Idle           Location
  *  0 ccon 0          idle            idle            00:12:54
  *  2 vty 0          idle            200.200.200.1
Internet>
Internet>

```

Nossa política de NAT ficou assim:

Firepower Management Center
Devices / NGFW NAT Policy Editor

LAB-NAT-Policy

Enter Description

Rules

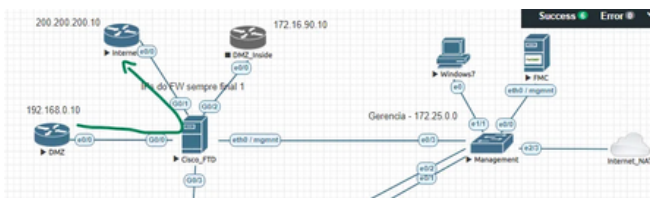
Filter by Device

#	Direction	Type	Source	Destination	Original Packet			Translated Packet			Options	
					Original Source	Original Destination	Original Service	Translated Source	Translated Destination	Translated Service		
Auto NAT Rules												
#		S...	ZONE-DMZ	ZONE-INTER	HOST_192.168.0			HOST_200.200.21			Dir true	
#		D...	ZONE-DMZ-F	ZONE-INTER	NET_172.16.0-0			Interface			Dir true	
NAT Rules After												



PARTE 2

Essa é nossa topologia (idem da primeira parte). **Faremos um NAT da DMZ para a Internet.** Observem apenas esses dois eqtos na figura abaixo.



Agora vejam a configuração de rotas do router da DMZ: apenas localmente conectadas. **Não há rota estática.**

```
DMZ
DMZ#show ip int brise | i
Ethernet0/0 192.168.0.10 YES NVRAM up up
DMZ#
DMZ#
DMZ#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       * - replicated route, % - next hop override

Gateway of last resort is not set

C 192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
  C 192.168.0.0/24 is directly connected, Ethernet0/0
  L 192.168.0.10/32 is directly connected, Ethernet0/0
DMZ#
```

E agora para o router da Internet, idem.

```
Internet
Internet#
Internet#
Internet#
Internet#
Internet#show ip int brise | i up
Ethernet0/0 200.200.200.10 YES NVRAM up up
Internet#
Internet#
Internet#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       * - replicated route, % - next hop override

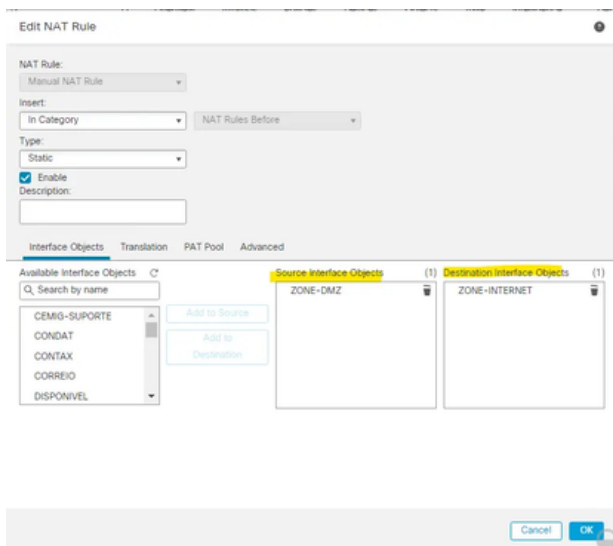
Gateway of last resort is not set

C 200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks
  C 200.200.200.0/24 is directly connected, Ethernet0/0
  L 200.200.200.10/32 is directly connected, Ethernet0/0
Internet#
```



Temos então um firewall interligando a rede DMZ e a rede Internet que **não sabem como chegar um no outro**.

Nosso objetivo prático é da DMZ dar um telnet no router Internet.



Vamos criar uma regra de **Manual NAT**, que iniciamos a falar dela na parte 1, com origem da DMZ para a Internet e iremos manipular o tráfego dessa forma:

O IP Real do router de Internet é 200.200.200.10, então, à partir do router da DMZ, vamos tratar o pacote original.



Da DMZ nossa origem é o 192.168.0.10 e o destino não pode ser na rede 200, já que não conhecemos essa rede. Então, o destino será um novo IP, o 192.168.0.9 — aqui o firewall faz proxy-arp desse IP nessa interface (no caso a DMZ). **De forma básica, à partir desse momento o IP .9 “começa a existir” na rede e quem responde por ele é o firewall.**

The screenshot shows the 'Add NAT Rule' configuration window. The 'Original Packet' section is highlighted with a red box. It contains the following fields:

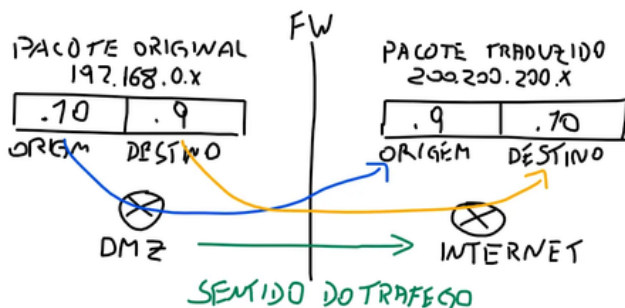
- Original Source: HOST_192.168.0.10
- Original Destination: Address (with HOST_192.168.0.9 selected)
- Original Source Port: (empty)
- Original Destination Port: (empty)

The 'Translated Packet' section contains the following fields:

- Translated Source: Address
- Translated Destination: HOST_200.200.200.10
- Translated Source Port: (empty)
- Translated Destination Port: (empty)

Após o pacote atravessar o Firepower, o IP que antes era 192.168.0.10, irá virar 200.200.200.9 (essa parte é como um NAT tradicional de origem, ou Auto NAT pra nós da Cisco), e o destino do pacote, ao invés de 192.168.0.9, será o 200.200.200.10.





Finalmente, apenas para verificação, vejam os MAC-ADDRESSES de cada um dos IPs envolvidos. A telinha preta no fundo é o SSH do firewall e o IP e MAC das duas interfaces envolvidas. Reparem nos MACs dos IPs nos dois switches ;)

```

DMZ
User Access Verification

Passwords
Internet#who
Line          User             Host(s)         Idle           Location
* 0 con 0      idle             00:06:41
* 2 vty 0      idle             00:00:00 200.200.200.9

Interface      User             Mode            Idle           Peer Address
Internet#sh arp
Internet#sh arp
Protocol  Address          Age (min)  Hardware Addr  Type   Interface
Internet 200.200.200.1   -          5001.0001.0002  ARPA   Ethernet0/0
Internet 200.200.200.9   2          5001.0001.0002  ARPA   Ethernet0/0
Internet 200.200.200.10  -          aabb.c000.1300  ARPA   Ethernet0/0
Internet#
Internet#exit
(Connection to 192.168.0.9 closed by foreign host)
Internet#show arp
Protocol  Address          Age (min)  Hardware Addr  Type   Interface
Internet 192.168.0.1     12         5001.0001.0002  ARPA   Ethernet0/0
Internet 192.168.0.9   4          5001.0001.0001  ARPA   Ethernet0/0
Internet 192.168.0.10  -          aabb.c000.0f00  ARPA   Ethernet0/0
Internet#
> show interface 1
Name: Ethernet0/0
MAC address 5001.0001.0002, MTU 1500
IP address 192.168.0.1, subnet mask 255.255.255.0
MAC address 5001.0001.0002, MTU 1500
IP address 200.200.200.1, subnet mask 255.255.255.0
MAC address 5001.0001.0001, MTU 1500
IP address 172.16.0.2, subnet mask 255.255.255.0
MAC address 5001.0001.0004, MTU 1500
IP address unassigned
  
```



AGRADECIMENTOS

Gostaria de agradecer a todos os leitores e seguidores do blog TechRebels nesses anos todos. Foi sensacional ter tido a chance de conhecer alguns pessoalmente.

Espero que o conteúdo possa ajudar muito mais profissionais a melhorarem e crescerem profissionalmente.

Se você recebeu esse ebook de um amigo, dê uma olhada nos treinamentos que temos disponíveis no ciberseguranca.cisco.com.br.

Grande abraço e muito sucesso!!!



 [linkedin.com/in/fmp7/](https://www.linkedin.com/in/fmp7/)

