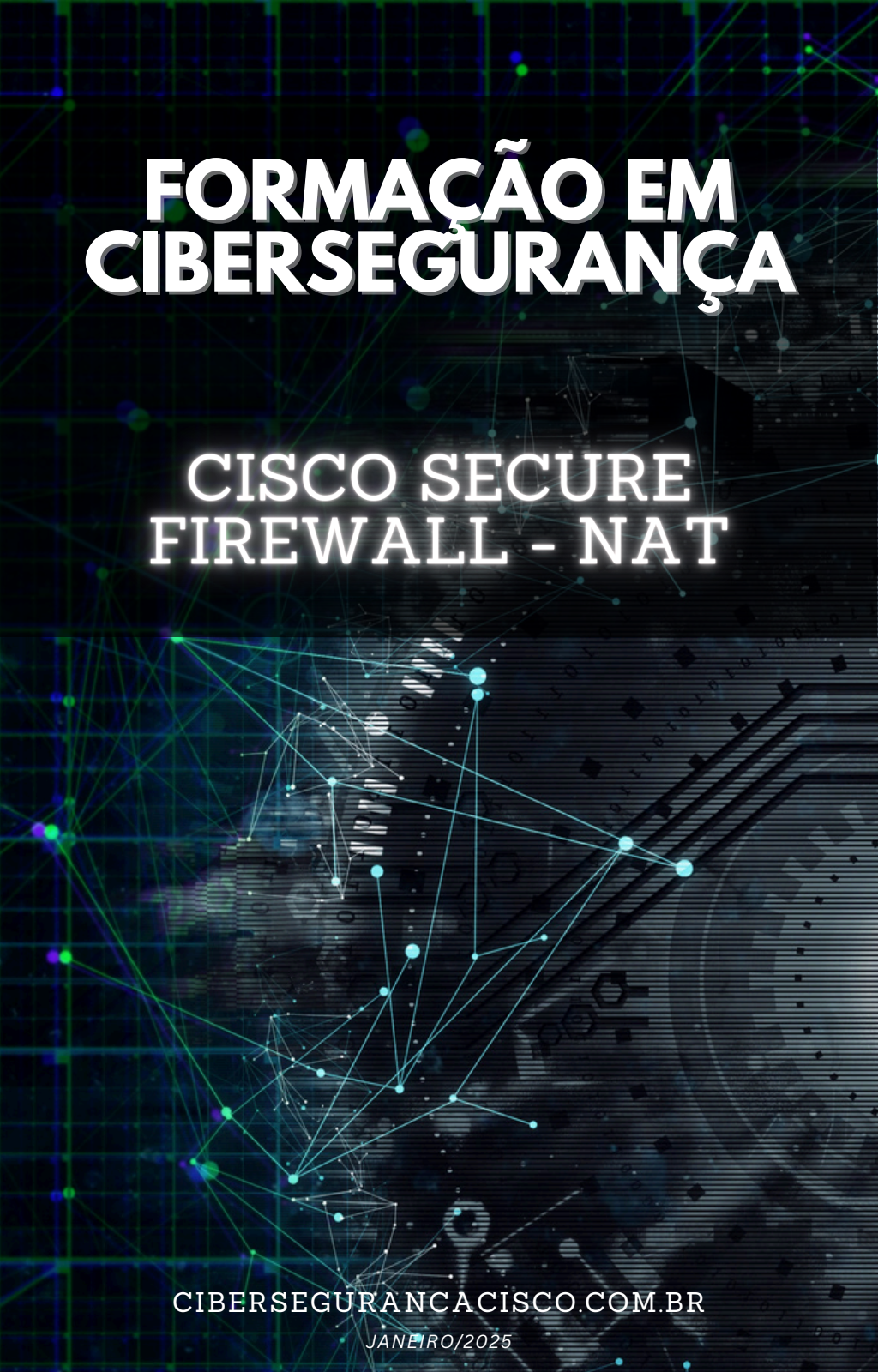
FORMAÇÃO EM CIBERSEGURANÇA

CISCO SECURE FIREWALL - NAT



CIBERSEGURANCACISCO.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

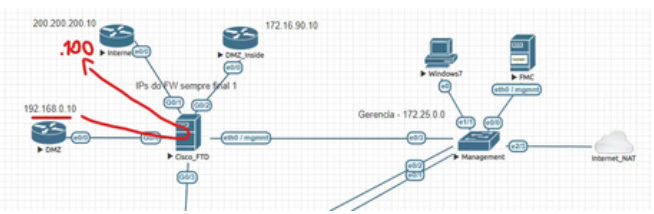
Até a versão **8.2 do ASA**, havia somente uma versão de NAT disponível — com algumas variações na sua aplicação. À partir da 8.3, a Cisco incluiu uma possibilidade adicional.

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.

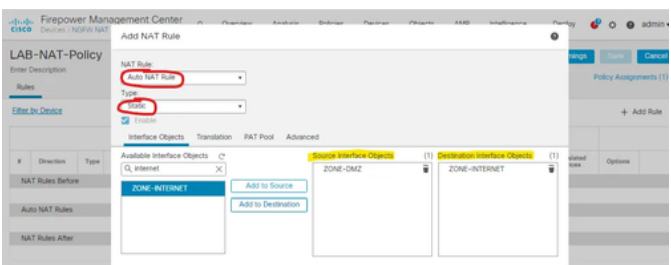
Obs: Os IPs das interfaces do FW são sempre final .1



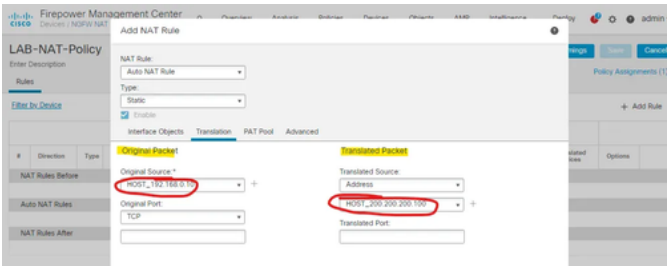
Imaginando o FW como uma parede, pensamos que o IP 192.168.0.10, ao atravessar a parede, virará um outro IP, no caso o 200.200.200.100.

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

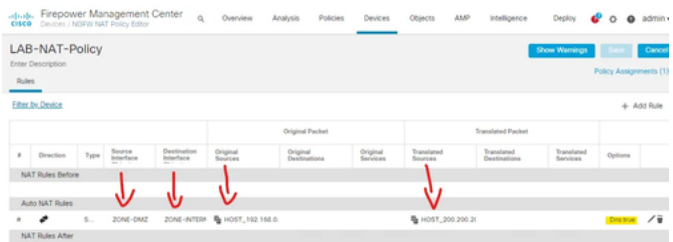
Na imagem abaixo, repare na regra de NAT e no tipo dele em vermelho. Já o amarelo, mostra a interface de origem e a de destino.



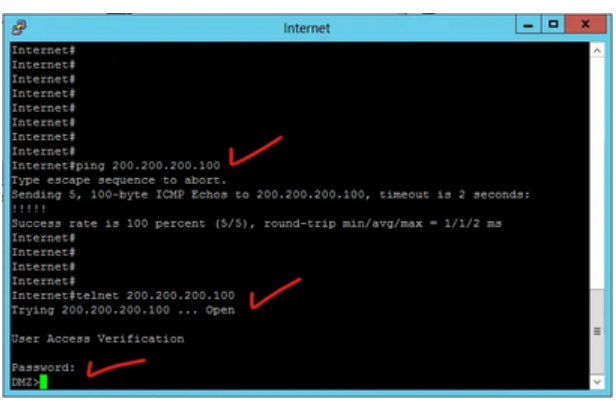
Abaixo, repare no pacote original, com o IP 192.168.0.10 e o pacote traduzido 200.200.200.100.



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.

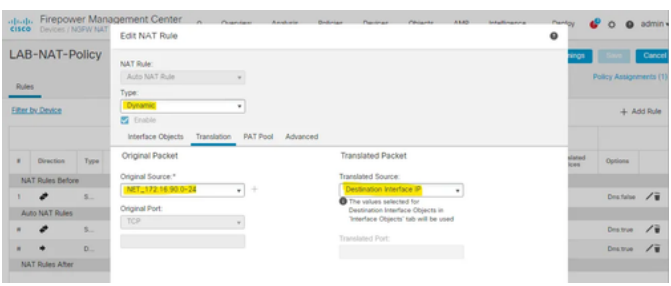


No router de Internet, conseguimos pingar o 200.200.200.100 e ao dar telnet, acessamos o router da DMZ.

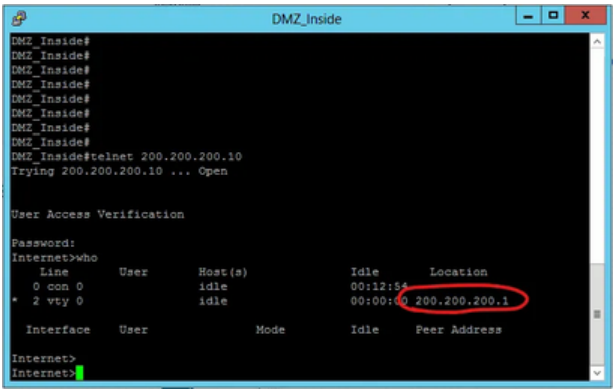


Esse tipo de NAT traduz a origem da requisição, e ele é indicado pela Cisco para os casos **simples** de tradução de IP, como por exemplo ao acessarmos a Internet. Da mesma forma poderíamos traduzir uma rede para o IP da interface externa do firewall, fazendo dessa forma um **PAT — Port Address Translation**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

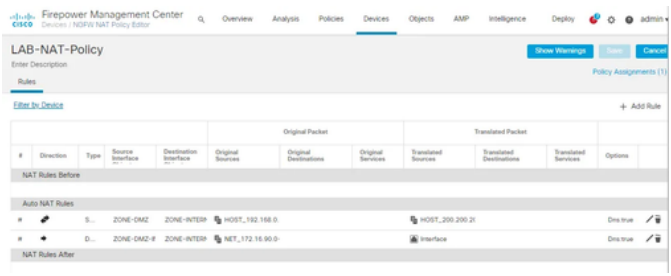
Veja na figura abaixo como ficaria: O tipo de NAT é dinâmico, e a origem é toda a rede da DMZ_Inside. O destino é o IP da interface de destino, no caso, a interface internet.



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.

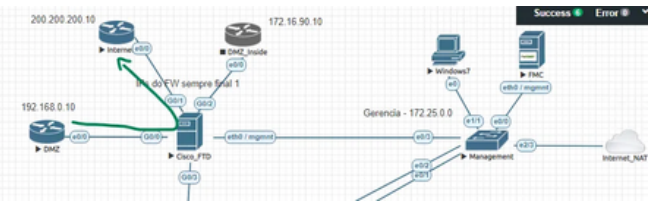


Nossa política de NAT ficou assim:



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.

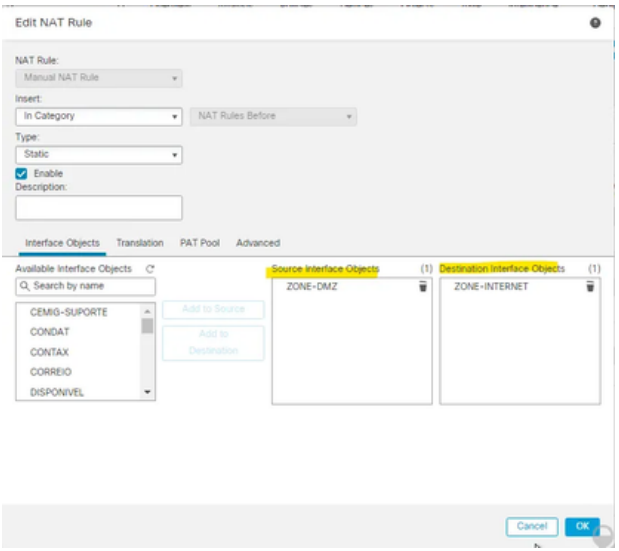


Agora vejam a configuração de rotas do router da DMZ: apenas localmente conectadas. **Não há rota estática.**

E agora para o router da Internet, idem.

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

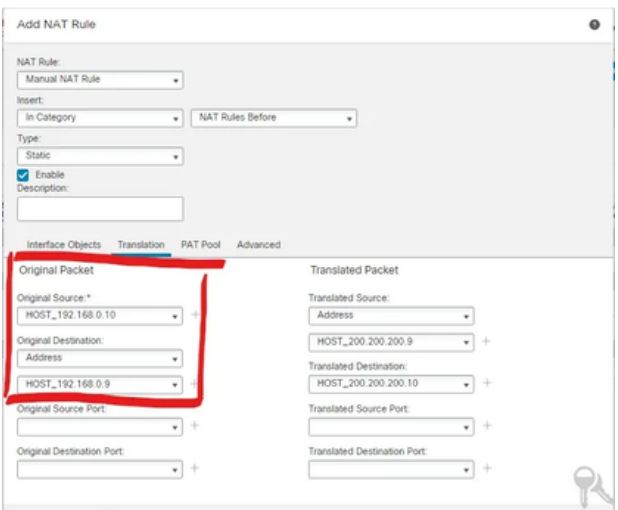
Nosso objetivo prático é da DMZ dar um telnet no router Internet.



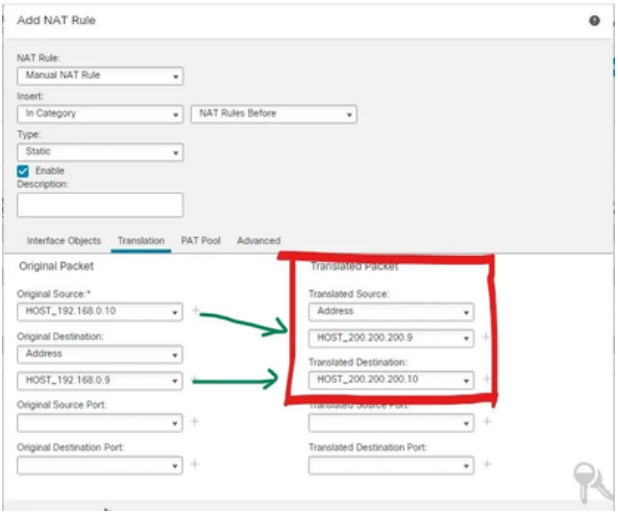
Vamos criar uma regra de **Manual NAT**, que iniciamos a falar dela na parte 1, com origem da DMZ para a Internet e iremos manipular o tráfego dessa forma:

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

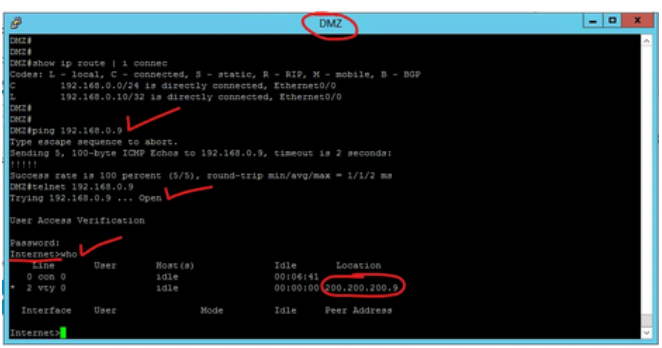
Da DMZ nossa origem é o 192.168.0.10 e o destino não pode ser na rede 200, já que não conhecemos essa rede. Então, o destino será um novo IP, o 192.168.0.9 — aqui o firewall faz proxy-arp desse IP nessa interface (no caso a DMZ). **De forma básica, à partir desse momento o IP .9 "começa a exitir" na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



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.

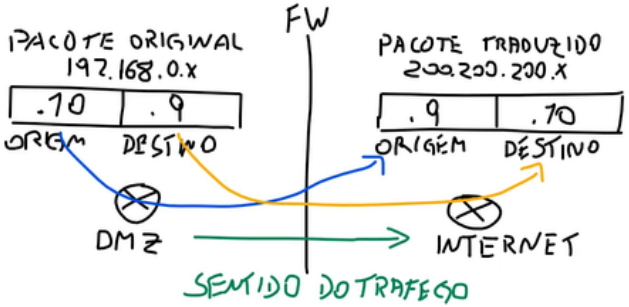


Feito o deploy da política, vamos testar. À partir do router da DMZ, vejam:



Nós demos telnet no IP 192.168.0.9 e, ao atravessarmos o firewall, nós chegamos no IP 200.200.200.10 com o IP 200.200.200.9

De forma prática, esse desenho ilustra o que aconteceu.



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 ;)

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/