Configurar Hairpin com o Firepower Management Center

Contents

Introdução

Este documento descreve as etapas necessárias para configurar corretamente o Hairpin em um Firepower Threat Defense (FTD) com o Firepower Management Center (FMC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Management Center (FMC)
- Defesa contra ameaças do Firepówer (FTD)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Management Center Virtual 7.2.4.
- Firepower Threat Defense Virtual 7.2.4.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

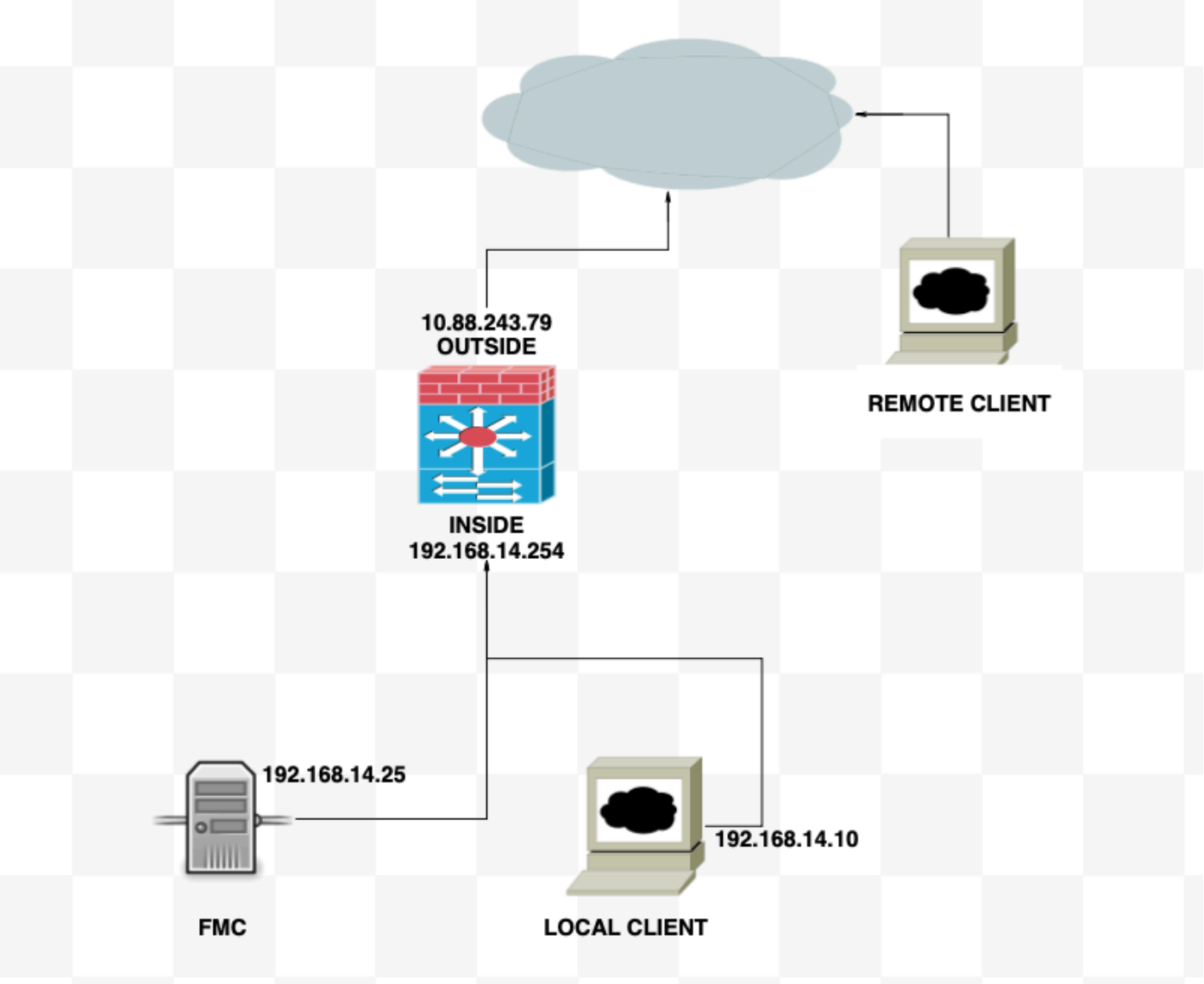
Configurar

O termo hairpin é usado porque o tráfego do cliente o torna para o roteador (ou firewall que implementa NAT) e é então retornado como um hairpin para a rede interna após a conversão para acessar o endereço IP privado do servidor.

Essa função é útil para serviços de rede como hospedagem na Web dentro de uma rede local, onde os usuários na rede local precisam acessar o servidor interno usando o mesmo URL ou endereço IP que os usuários externos usariam. Ele garante acesso uniforme aos recursos, independentemente de a solicitação se originar de dentro ou de fora da rede local.

Neste exemplo, um FMC deve ser acessado através do IP da interface externa do FTD

Diagrama

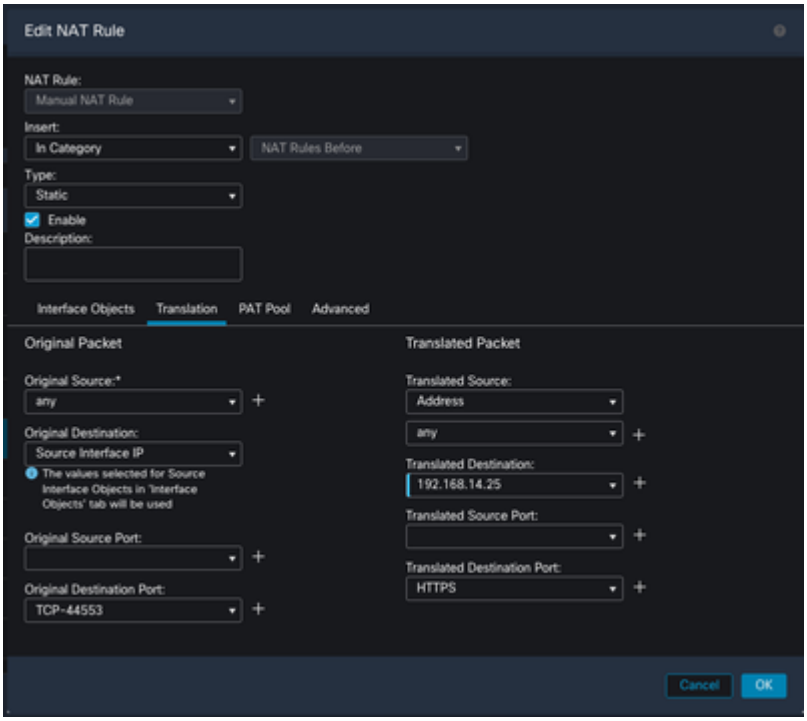


Etapa 1. Configurar O Nat Externo

Como primeira etapa, um NAT estático deve ser configurado; neste exemplo, o IP de destino e a porta de destino são convertidos usando o IP da interface externa e o destino da porta é 44553.

No FMC, navegue até Device > NAT para criar ou editar a política existente e clique na caixa Add Rule.

- Regra NAT: Regra Nat Manual
- Fonte original: qualquer um
- Destino original: IP da interface de origem
- Porta de destino original: 44553
- Destino traduzido: 192.168.14.25
- Porta de destino convertida: 443



Configure a política. Navegue até Policies > Access Control para criar ou editar a política existente e clique na caixa Add Rule.

Zona de Origem: Externa

Zona de destino: Interna

Rede de Origem: qualquer um

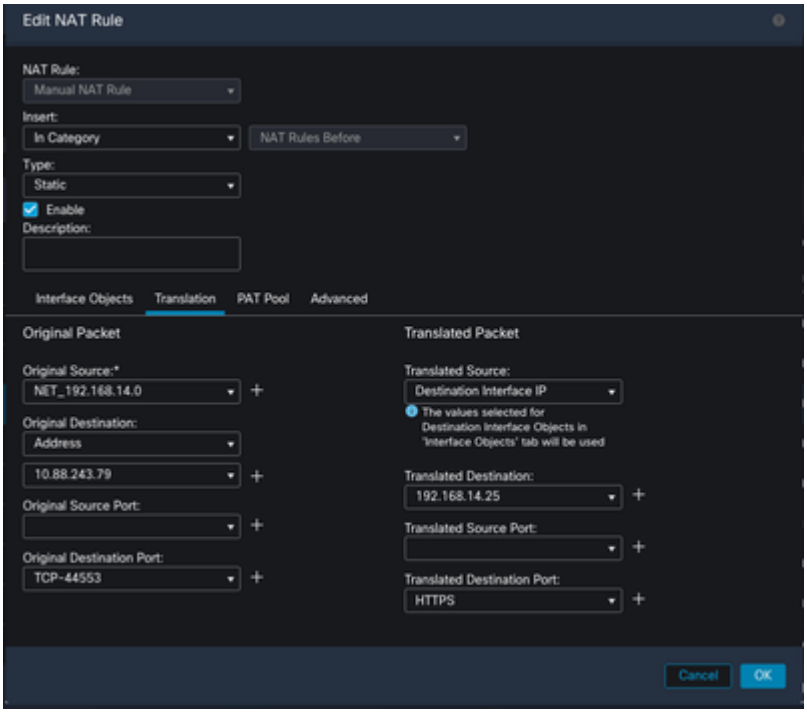
Rede de destino: 10.88.243.79

Etapa 2. Configurar O Nat Interno (Hairpin)

Como segunda etapa, um NAT estático deve ser configurado de dentro para dentro; neste exemplo, o IP de destino e a porta de destino são convertidos usando um objeto com o IP da interface externa e a porta de destino é 44553.

No FMC, navegue até Device > NAT para editar a política existente e clique na caixa Add Rule.

- Regra NAT: Regra Nat Manual
- Fonte original: 192.168.14.0/24
- Destino original: Endereço 10.88.243.79
- Porta de destino original: 44553
- Fonte traduzida: IP da interface de destino
- Destino traduzido: 192.168.14.25
- Porta de destino convertida: 443



Configure a política. Navegue até Policies > Access Control para editar a política existente e clique na caixa Add Rule.

Zona de Origem: qualquer um

Zona de destino: qualquer um

Rede de Origem: 192.168.14.0/24

Rede de destino: 10.88.243.79

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks
Mandatory - la primera (1-4)					
1	nat-fmc	OUTSIDE	INSIDE	any	*Any*
2	Hairpin	*Any*	*Any*	NET_192.168.14	10.88.243.79

Verificar

A partir do cliente local, execute um telnet com o IP de destino e a porta de destino:

Se esta mensagem de erro "telnet incapaz de se conectar ao host remoto: Connection timed out" prompt, algo deu errado em algum momento durante a configuração.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
telnet: Unable to connect to remote host: Connection timed out
```

Mas, se a mensagem Connected (Conectado) for exibida, a configuração foi bem-sucedida.

```
┌──(root💀 kali)-[/home/kali]
└─# telnet 10.88.243.79 44553
Trying 10.88.243.79 ...
Connected to 10.88.243.79.
Escape character is '^]'.
```

Troubleshooting

Se você estiver tendo problemas com a Tradução de Endereço de Rede (NAT), use este guia passo a passo para solucionar problemas comuns.

Passo 1: Verificação de Configuração de Regras de NAT

- Revisar regras de NAT: Verifique se todas as regras de NAT estão configuradas corretamente no FMC. Verifique se os endereços IP origem e destino, bem como as portas, são precisos.
- Atribuição de interface: Confirme se as interfaces de origem e destino estão atribuídas corretamente na regra NAT. O mapeamento incorreto pode fazer com que o tráfego não seja convertido ou roteado corretamente.
- Prioridade da regra NAT: Verifique se a regra NAT está posicionada na parte superior de

qualquer outra regra que possa corresponder ao mesmo tráfego. As regras no FMC são processadas em ordem sequencial, portanto, uma regra colocada acima tem precedência.

Passo 2: Verificação de regras de controle de acesso (ACL)

- Revise as ACLs: Verifique as Access Control Lists (Listas de controle de acesso) para certificar-se de que elas são apropriadas para permitir o tráfego NAT. As ACLs devem ser configuradas para reconhecer os endereços IP traduzidos.
- Ordem das regras: Verifique se a lista de controle de acesso está na ordem correta. Como as regras de NAT, as ACLs são processadas de cima para baixo, e a primeira regra que corresponde ao tráfego é a que é aplicada.
- Permissões de tráfego: Verifique se existe uma lista de controle de acesso apropriada para permitir o tráfego da rede interna para o destino convertido. Se uma regra estiver ausente ou configurada incorretamente, o tráfego desejado poderá ser bloqueado.

Passo 3: Diagnósticos adicionais

- Usar ferramentas de diagnóstico: Utilize as ferramentas de diagnóstico disponíveis no FMC para monitorar e depurar o tráfego que passa pelo dispositivo. Isso inclui a exibição de logs em tempo real e eventos de conexão.
- Reiniciar Conexões: Em alguns casos, as conexões existentes não podem reconhecer as alterações feitas nas regras de NAT ou nas ACLs até que sejam reiniciadas. Considere limpar as conexões existentes para forçar a aplicação de novas regras.

Do LINA:

<#root>

firepower#

clear xlate

- Verificar tradução: Use comandos como show xlate e show nat na linha de comando se estiver trabalhando com dispositivos FTD para verificar se as conversões de NAT estão sendo executadas como esperado.

Do LINA:

<#root>

firepower#

show nat

<#root>

```
firepower#
 show xlate
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.