Configurar Hairpin no ASA

Contents

Introdução

Este documento descreve as etapas necessárias para configurar corretamente o Hairpin em um Cisco Adaptive Security Appliance (ASA)

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Configuração de NAT no ASA
- Configuração da ACL no ASA

Componentes Utilizados

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

- Software Cisco Adaptive Security Appliance Versão 9.18(4)22

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

A Conversão de Endereço de Rede (NAT - Network Address Translation) Hairpin, também conhecida como loopback NAT ou reflexão NAT, é uma técnica usada no roteamento de rede pela qual um dispositivo em uma rede privada pode acessar outro dispositivo na mesma rede privada através de um endereço IP público.

Isso é usado quando um servidor é hospedado atrás de um roteador e você deseja permitir que os dispositivos na mesma rede local do servidor acessem-no usando o endereço IP público (aquele atribuído ao roteador pelo Provedor de Serviços de Internet), como um dispositivo externo faria.

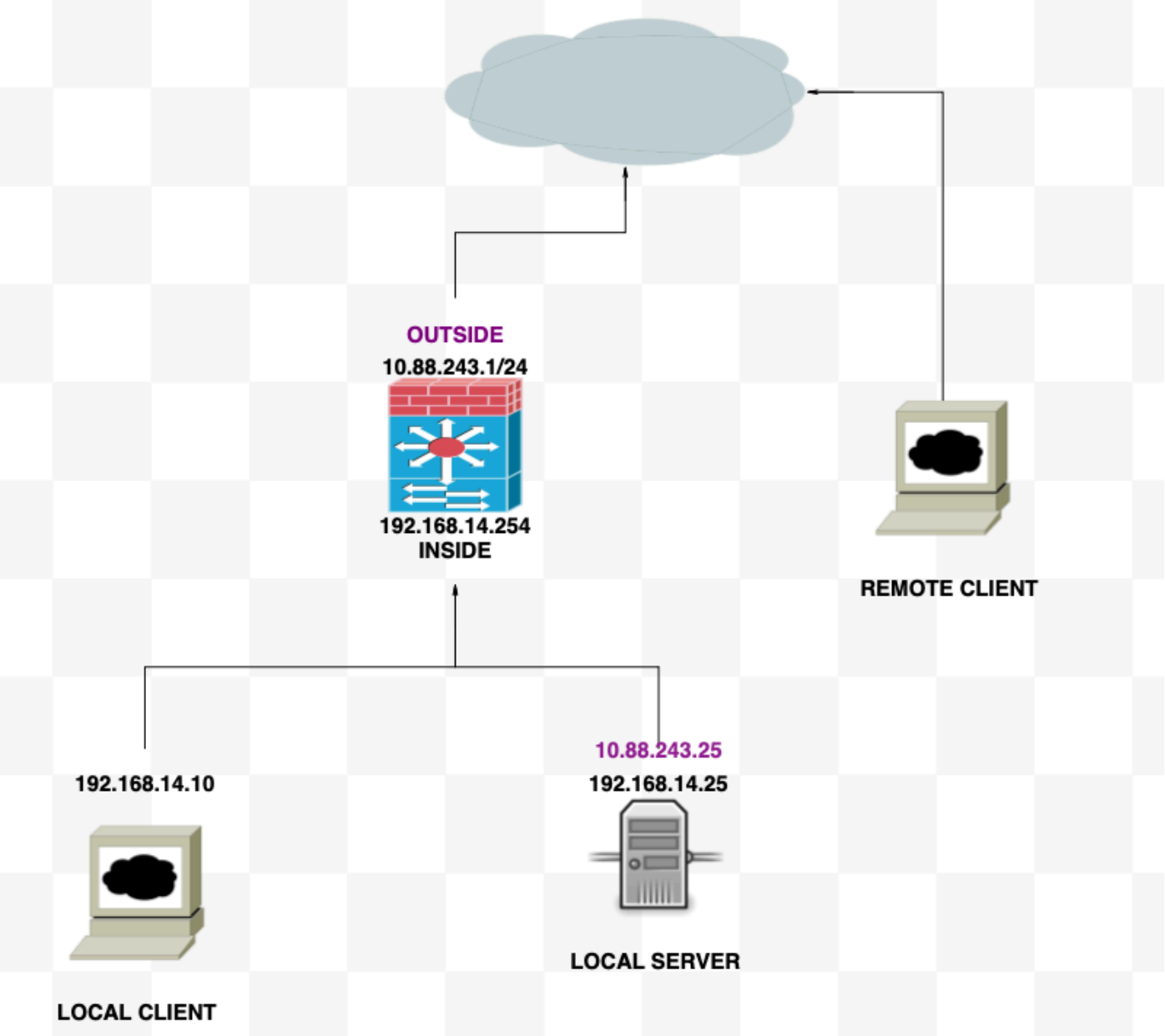
O termo "hairpin" é usado porque o tráfego do cliente o torna para o roteador (ou firewall que implementa NAT) e é então "devolvido" como um hairpin para a rede interna após a conversão para acessar o endereço IP privado do servidor.

Por exemplo, você tem um servidor Web na rede local com um endereço IP privado. Você deseja acessar esse servidor usando seu endereço IP público ou um nome de domínio que seja resolvido para o endereço IP público, mesmo quando você estiver na mesma rede local.

Sem o Hairpin NAT, o roteador não entenderia essa solicitação, pois espera que as solicitações para o endereço IP público venham de fora da rede.

O Hairpin NAT resolve esse problema permitindo que o roteador reconheça que, embora a solicitação esteja sendo feita para um IP público, ela precisa ser roteada para um dispositivo na rede local.

Diagrama de Rede



Configurações

Etapa 1. Criar os Objetos

- Rede interna:192.168.14.10
- Servidor Web: 192.168.14.25
- Servidor Web público: 10.88.243.25
- Porta: 80

<#root>

```
ciscoasa(config)#
 object network Local_Client
ciscoasa(config-network-object)#
 host 192.168.14.10
```

```
ciscoasa(config)#
 object network Web_Server
ciscoasa(config-network-object)#
 host 192.168.14.25
ciscoasa(config)#
 object network P_Web_Server
ciscoasa(config-network-object)#
 host 10.88.243.25
ciscoasa(config)#
 object service HTTP
ciscoasa(config-service-object)#
 service tcp destination eq 80
```

Etapa 2. Crie o NAT

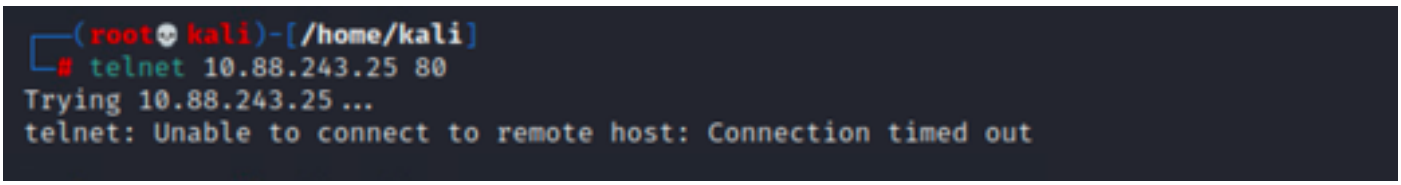
<#root>

```
ciscoasa
(config-service-object)# nat (Inside,Inside) source dynamic Local_Client interface destination static P_
```

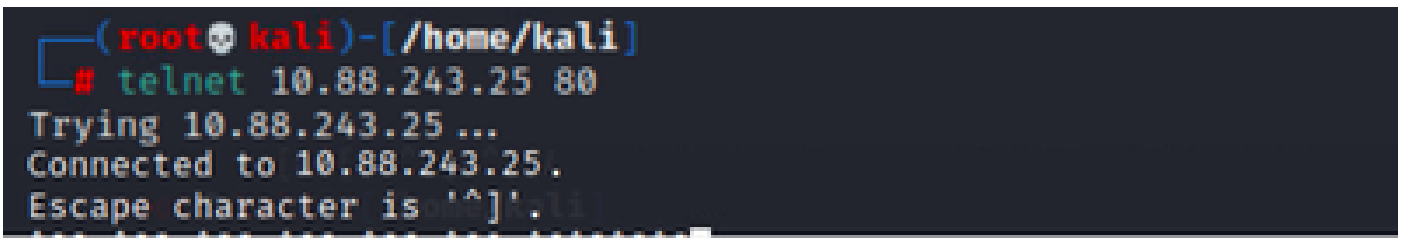
Verificar

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

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



Mas se disser "Conectado", funciona!



Troubleshooting

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

Etapa 1: Verificação da configuração das regras de NAT

- Revisar as regras de NAT: verifique se todas as regras de NAT estão configuradas corretamente. 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 corretamente atribuídas 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 tem prioridade mais alta do que qualquer outra regra que possivelmente corresponda ao mesmo tráfego. As regras são processadas em ordem sequencial, portanto, uma regra colocada acima tem precedência.

Etapa 2: Verificação das regras de controle de acesso (ACL)

- Revise as ACLs: Verifique as Listas de controle de acesso para certificar-se de que elas são apropriadas para permitir o tráfego de 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.

Etapa 3: Diagnósticos adicionais

- Usar ferramentas de diagnóstico: utilize as ferramentas de diagnóstico disponíveis 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 reconhecem as alterações feitas nas regras de NAT ou ACLs até que sejam reiniciadas. Considere limpar as conexões existentes para forçar a aplicação de novas regras.

<#root>

```
ciscoasa(config)#
 clear xlate
```

- Verificar tradução: use comandos como `show xlate` e `show nat` na linha de comando se

estiver trabalhando com dispositivos ASA para verificar se as conversões NAT estão sendo executadas como esperado.

```
<#root>

ciscoasa(config)#

 show xlate
```

```
<#root>

ciscoasa(config)#

 show nat
```

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.