在ASA上配置髮夾

目錄

簡介

本文檔介紹在思科自適應安全裝置(ASA)上成功配置髮夾的必要步驟。

必要條件

需求

思科建議您瞭解以下主題：

- ASA上的NAT配置
- ASA上的ACL配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科自適應安全裝置軟體版本9.18(4)22

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

髮夾網路位址翻譯(NAT)，也稱為NAT回送或NAT反射，是網路路由中使用的技術，使用此技術，私人網路上的裝置可以透過公用IP位址存取相同私人網路上的其他裝置。

當伺服器託管在路由器後方，並且您希望啟用與伺服器位於同一本地網路中的裝置使用公有IP地址（由網際網路服務提供商分配給路由器的地址）訪問它時，會使用這種方法，就像外部裝置一樣。

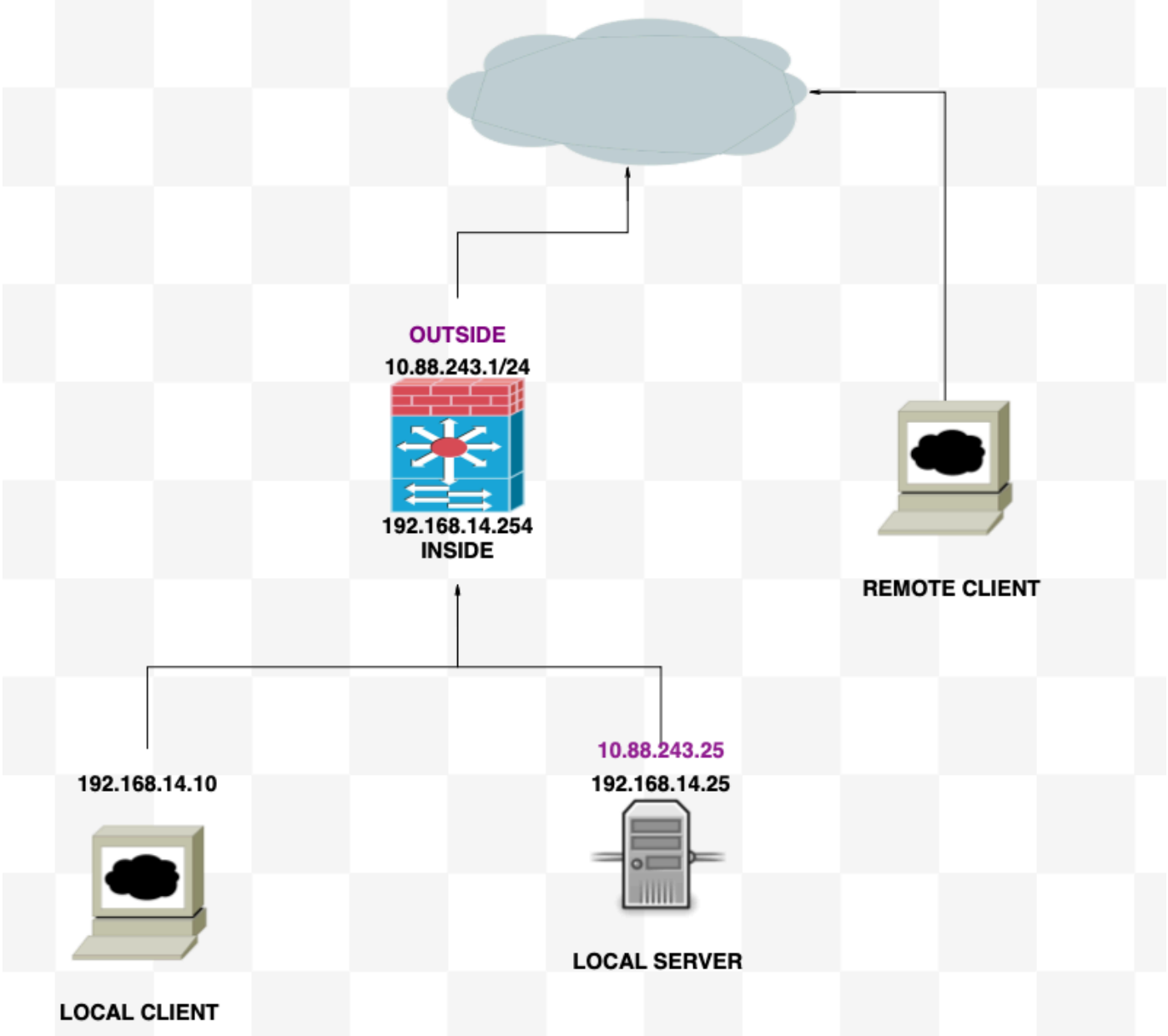
之所以使用髮夾這一術語，是因為來自客戶端的流量會發往路由器（或實施NAT的防火牆），然後在轉換後像髮夾一樣返回到內部網路，以訪問伺服器的專用IP地址。

例如，您的本地網路上有一個Web伺服器，該伺服器具有私有IP地址。您想要使用它的公用IP位址或解析為公用IP位址的網域名稱來存取此伺服器，即使您位於相同的本機網路中也是如此。

如果沒有Hairpin NAT，您的路由器將無法理解此請求，因為它預期對公共IP地址的請求來自網路外部。

髮夾型NAT透過允許路由器辨識儘管請求是傳送到公共IP，但需要將其路由到本地網路中的裝置來解決此問題。

網路圖表



組態

步驟 1.建立物件

- 內部網路：192.168.14.10
- Web伺服器：192.168.14.25
- 公共Web伺服器：10.88.243.25
- 連線埠：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
```

步驟 2.建立NAT

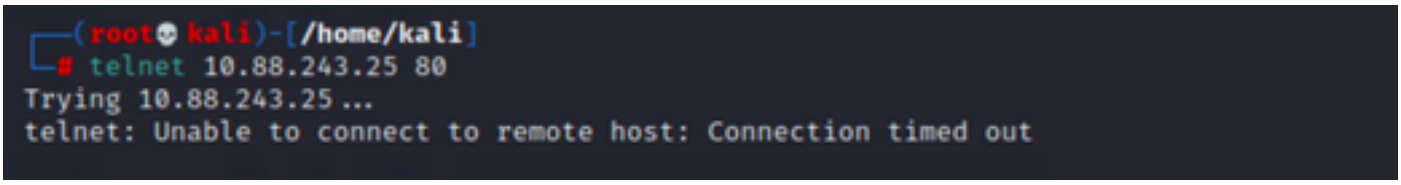
<#root>

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

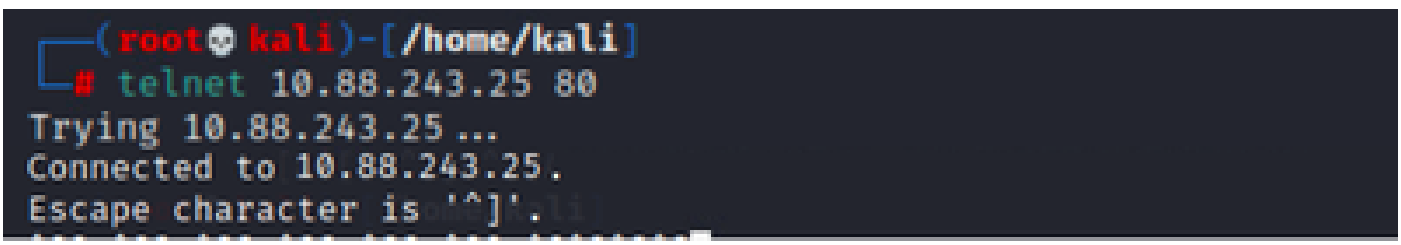
驗證

從本地客戶端使用目的埠執行telnet目的IP：

如果此消息「telnet unable to connect to remote host： Connection timed out」提示符，則在配置期間的某一時刻出錯。



但如果它顯示Connected，它就會起作用！



疑難排解

如果您遇到網路地址轉換(NAT)問題，請使用本分步指南排除常見問題故障。

第1步：NAT規則配置檢查

- 檢視NAT規則：確保所有NAT規則都配置正確。檢查源IP地址和目的IP地址以及埠是否正確。
- 介面分配：確認NAT規則中正確分配了源介面和目標介面。不正確的對映會導致無法正確轉換或路由流量。
- NAT規則優先順序：驗證NAT規則的優先順序是否高於可能匹配相同流量的任何其他規則。規則會依序處理，因此放在較高位置的規則具有優先順序。

步驟2：存取控制規則(ACL)驗證

- 檢視ACL：檢查訪問控制清單以確保它們適用於允許NAT流量。必須配置ACL才能辨識轉換後的IP地址。
- 規則順序：確保訪問控制清單的順序正確。與NAT規則一樣，ACL是從上到下進行處理，匹配流量的第一個規則是應用的規則。
- 流量許可權：驗證是否存在適當的訪問控制清單，以允許從內部網路到轉換目標的流量。如果缺少規則或規則配置不正確，可能會阻止所需的流量。

步驟3：其他診斷

- 使用診斷工具：利用可用的診斷工具來監控和調試透過裝置的流量。這包括檢視即時日誌和連線事件。
- 重新啟動連線：在某些情況下，現有連線在重新啟動之前無法辨識對NAT規則或ACL所做的更改。考慮清除現有連線以強制應用新規則。

<#root>

ciscoasa(config)#

clear xlate

- 驗證轉換：如果使用ASA裝置驗證NAT轉換是否按預期執行，請在命令列中使用show xlate和show nat等命令。

<#root>

ciscoasa(config)#

show xlate

<#root>

```
ciscoasa(config)#
 show nat
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。