排除ASA網路地址轉換(NAT)配置故障

目錄

簡介

本文檔介紹如何對思科自適應安全裝置(ASA)平台上的網路地址轉換(NAT)配置進行故障排除。

必要條件

需求

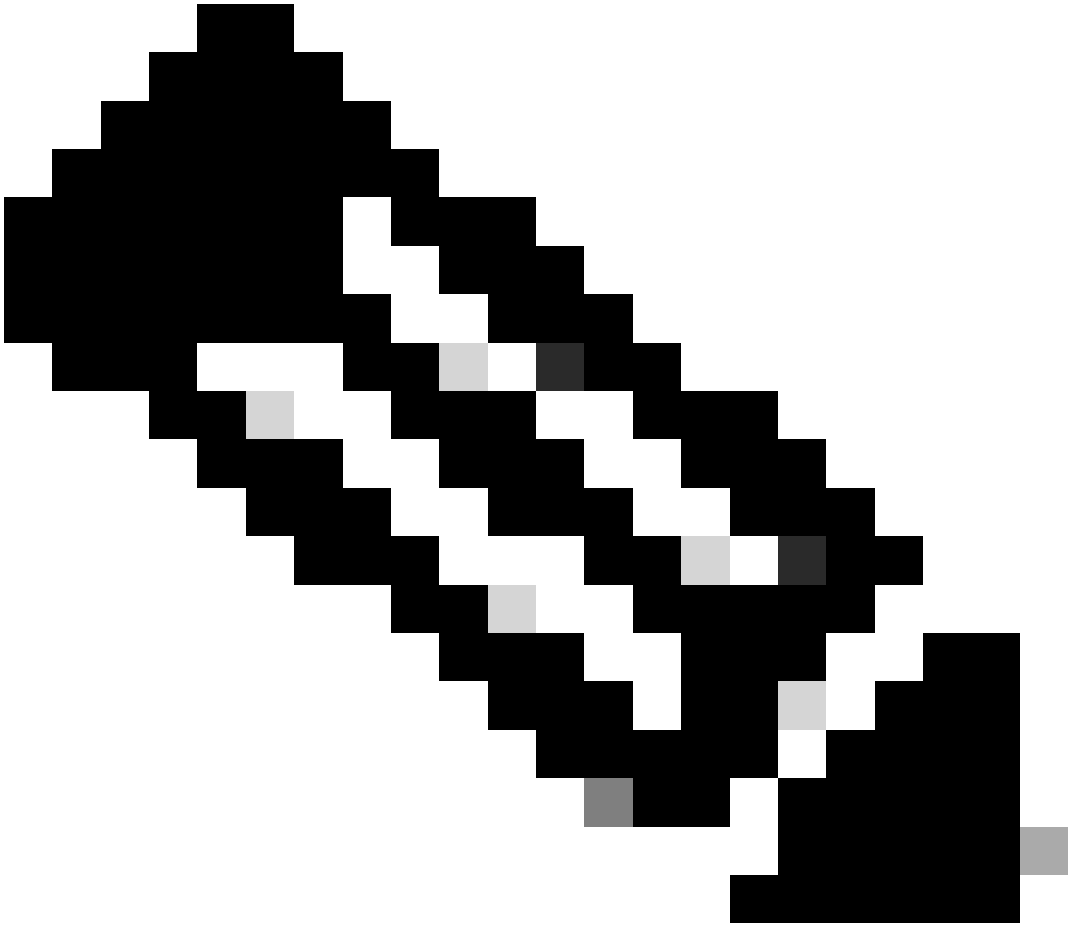
本文件沒有特定需求。

採用元件

本文檔中的資訊基於ASA版本8.3及更高版本。

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。

排除ASA上的NAT配置故障



注意：有關NAT配置的一些基本示例（包括顯示基本NAT配置的影片），請參閱本文檔底部的相關資訊部分。

當您排除NAT配置故障時，必須瞭解如何使用ASA上的NAT配置來構建NAT策略表。

這些配置錯誤是ASA管理員遇到的大多數NAT問題的原因：

- NAT配置規則順序混亂。例如，手動NAT規則放置在NAT表的頂部，這會導致在NAT表更深處放置的更具體的規則永遠不會被觸及。
- NAT配置中使用的網路對象過於廣泛，從而導致流量不慎與這些NAT規則匹配，並遺漏更特定的NAT規則。

Packet tracer實用程式可用於診斷ASA上大多數與NAT相關的問題。有關如何使用NAT配置來構建NAT策略表，以及如何排除和解決特定NAT問題的詳細資訊，請參閱下一節。

此外，還可以使用show nat detail命令來瞭解新連線所影響的NAT規則。

如何使用ASA配置構建NAT策略表

根據NAT表評估ASA處理的所有資料包。此評估從頂部（第1部分）開始，然後向下運行，直到NAT規則匹配。

通常，一旦匹配NAT規則，該NAT規則將應用到連線，並且不再針對資料包檢查更多NAT策略，但是有一些警告將在後面介紹。

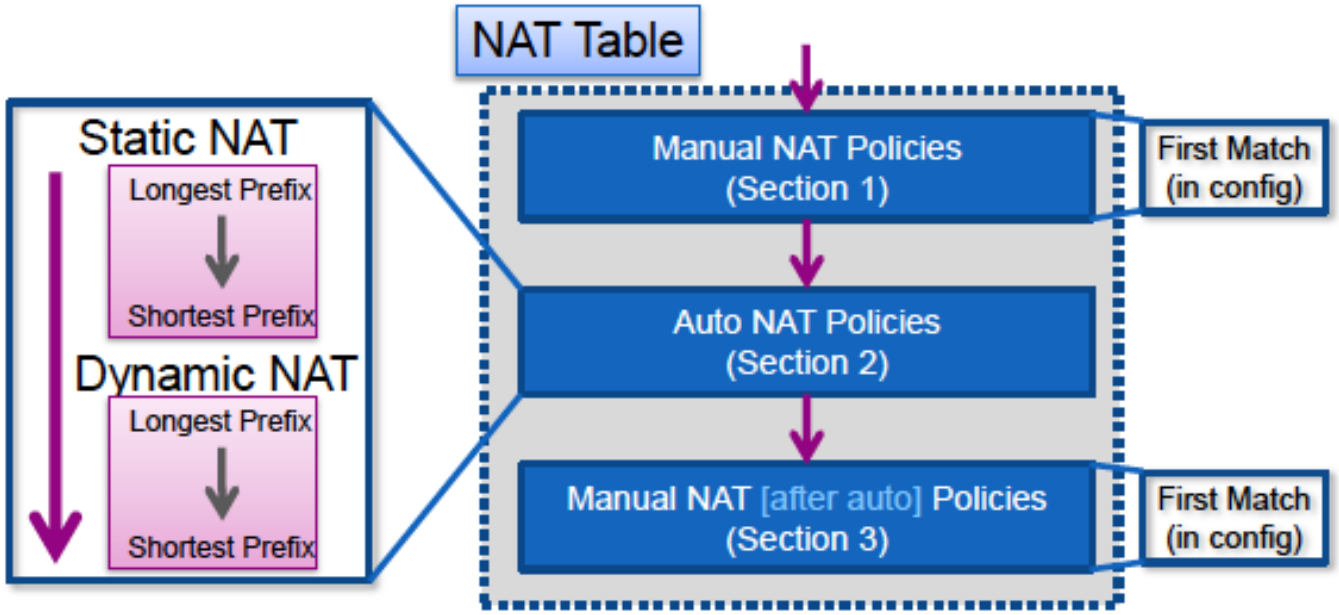
NAT策略表

ASA上的NAT策略是從NAT配置構建的。

ASA NAT表的三個部分是：

第1部分	手動NAT策略 系統會按照它們在配置中出現的順序來處理它們。
第2部分	自動NAT策略 根據對象中的NAT型別（靜態或動態）和字首（子網掩碼）長度來處理這些資訊。
第3部分	自動後手動NAT策略 系統會按照它們在配置中出現的順序來處理它們。

下圖顯示了不同的NAT部分及其順序：



NAT規則匹配

第1部分

- 首先根據以第一個規則開頭的NAT表的第1部分評估流量。
  - 如果資料包的源IP和目標IP與手動NAT規則的引數匹配，則會應用轉換並停止該過程，並且不會評估任何部分中的其他NAT規則。
  - 如果未匹配NAT規則，則會根據NAT表的第2部分評估流量。

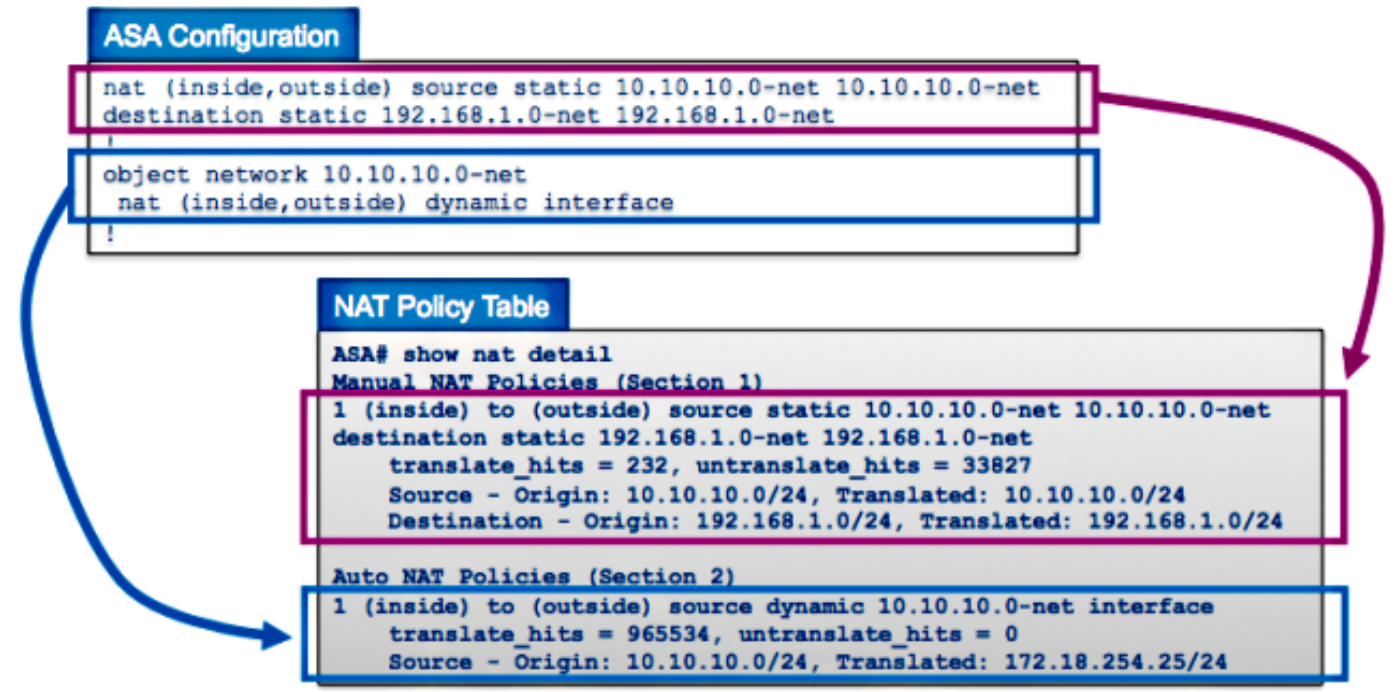
第2部分

- 根據第2部分NAT規則，按照前面指定的順序評估流，首先評估靜態NAT規則，然後評估動態NAT規則。
  - 如果轉換規則與流的源IP或目標IP匹配，則可以應用轉換，並繼續評估其餘規則，以檢視它們是否與流中的其他IP匹配。例如，一個自動NAT規則可以轉換源IP，另一個自動NAT規則可以轉換目標。
  - 如果流與自動NAT規則匹配，則當到達第2部分結尾時，NAT查詢將停止，並且不會計算第3部分中的規則。
  - 如果第2部分的NAT規則與流不匹配，則查詢將轉到第3部分

第3部分

- 第3節中的過程與第1節中的過程基本相同。 如果資料包的源IP和目標IP與手動NAT規則的引數匹配，則會應用轉換並停止該過程，並且不會評估任何部分中的其他NAT規則。

本示例展示如何在NAT表中顯示具有兩個規則（一個手動NAT語句和一個自動NAT配置）的ASA NAT配置：



如何排除NAT故障

使用Packet Tracer實用程式

要對NAT配置問題進行故障排除，請使用Packet Tracer實用程式驗證資料包是否符合NAT策略。Packet tracer允許您指定進入ASA的示例資料包，ASA指示對資料包應用什麼配置以及是否允許該配置。

在下一個示例中，給出了一個進入內部介面併發往Internet上主機的示例TCP資料包。Packet tracer實用程式顯示資料包與動態NAT規則匹配，並被轉換為外部IP地址172.16.123.4：

<#root>

ASA#

packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80

...(output omitted)...

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:

object network 10.10.10.0-net
nat (inside,outside) dynamic interface

Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

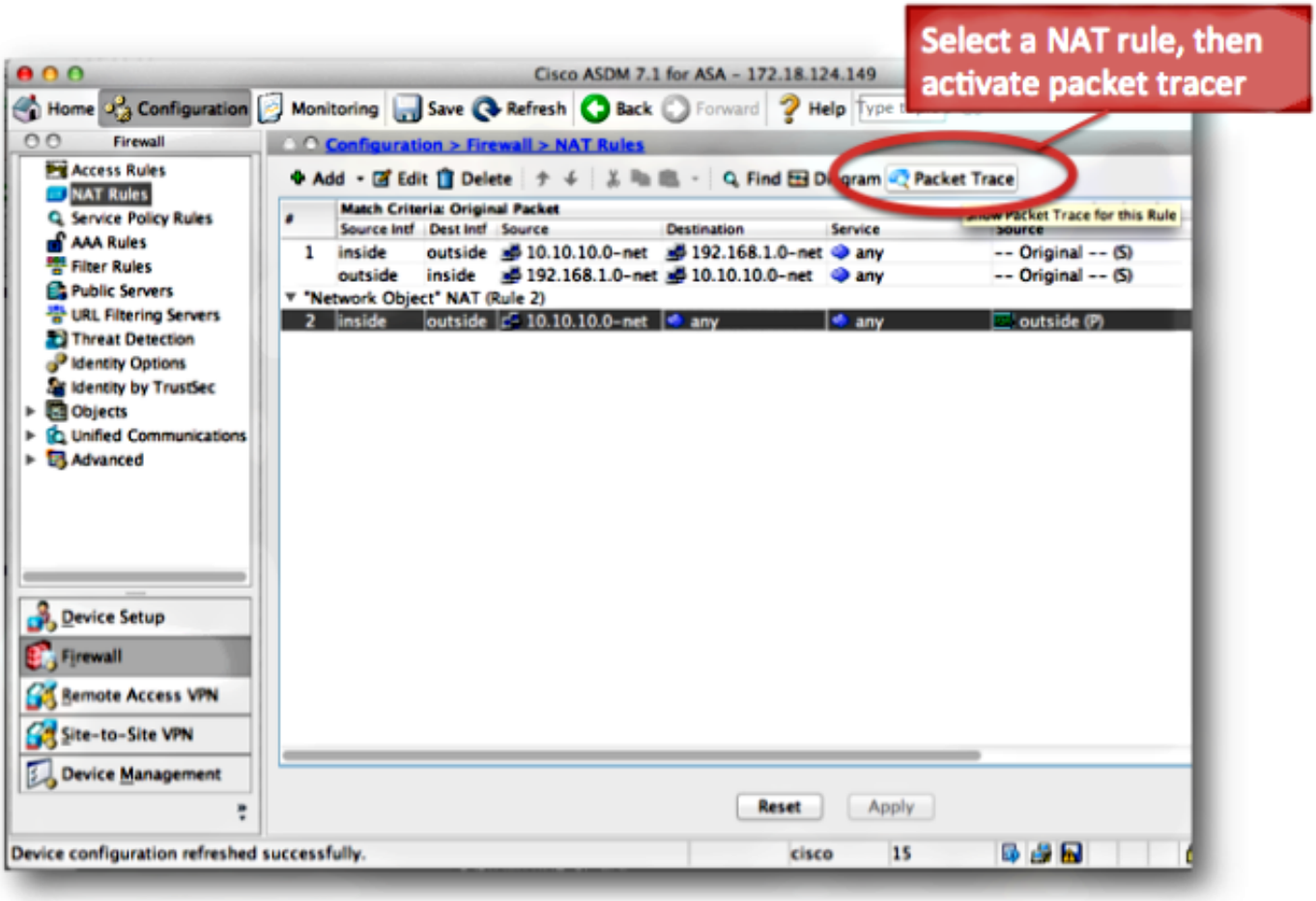
...(output omitted)...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up

Action: allow

ASA#

選擇NAT規則並按一下Packet Trace以從思科自適應安全裝置管理器(ASDM)啟用Packet Tracer。這將使用NAT規則中指定的IP地址作為Packet Tracer工具的輸入：

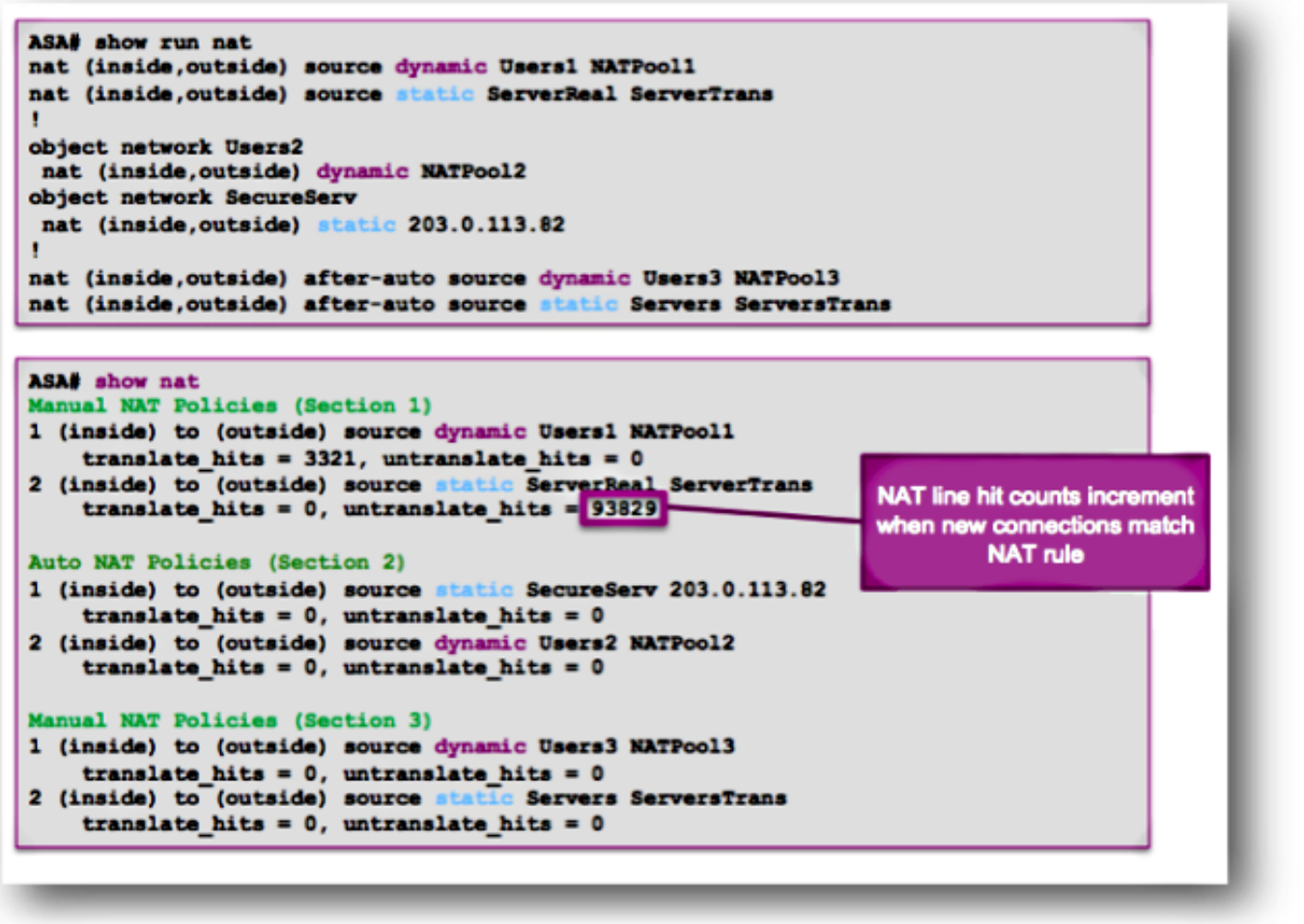


檢視Show Nat命令的輸出

show nat detail命令的輸出可用於檢視NAT策略表。具體而言，可以使用translate_hits和untranslate_hits計數器確定ASA上使用的NAT條目。

如果您看到新的NAT規則沒有translate_hits或untranslate_hits，則意味著資料流不會到達ASA，或者NAT表中優先順序更高的其他規則可能與資料流匹配。

以下是來自其他ASA配置的NAT配置和NAT策略表：



在上一個示例中，在該ASA上配置了六個NAT規則。show nat輸出顯示如何使用這些規則構建NAT策略表，以及每個規則的translate_hits和untranslate_hits數。

這些命中的計數器每次連線僅增加一次。在透過ASA建立連線後，與該當前連線匹配的後續資料包不會增加NAT線路（很像訪問清單命中計數在ASA上的工作方式）。

Translate_hits：向前方向與NAT規則匹配的新連線數。

「轉發方向」表示連線是透過ASA在NAT規則中指定的介面方向上構建的。

如果NAT規則指定將內部伺服器轉換為外部介面，則NAT規則中介面的順序為「nat (inside，outside)……」；如果該伺服器發起到外部主機的新連線，translate_hit計數器將會增加。

Untranslate_hits：與NAT規則反向匹配的新連線數。

如果NAT規則指定將內部伺服器轉換為外部介面，則NAT規則中介面的順序為「nat (inside，outside)……」；如果ASA外部的客戶端發起到內部伺服器的新連線，untranslate_hit計數器將會增加。

同樣，如果您看到新的NAT規則沒有translate_hits或untranslate_hits，則這意味著流量不會到達ASA，或者可能在NAT表中具有更高優先順序的另一個規則與該流量匹配。

NAT問題故障排除方法

使用Packet Tracer確認示例資料包是否與ASA上的正確NAT配置規則匹配。使用show nat detail命令以瞭解所命中的NAT策略規則。如果連線匹配的NAT配置與預期不同，請使用以下問題進行故障排除：

- 是否有其他NAT規則優先於您希望流量命中的NAT規則？
- 是否存在另一個NAT規則，其對象定義太寬（子網掩碼太短，例如255.0.0.0），從而導致此資料流與錯誤的規則匹配？
- 手動NAT策略是否順序混亂，從而導致資料包匹配錯誤的規則？
- 您的NAT規則配置是否不正確，從而導致規則與您的流量不匹配？

有關問題和解決方案的示例，請參見下一節。

NAT配置的常見問題

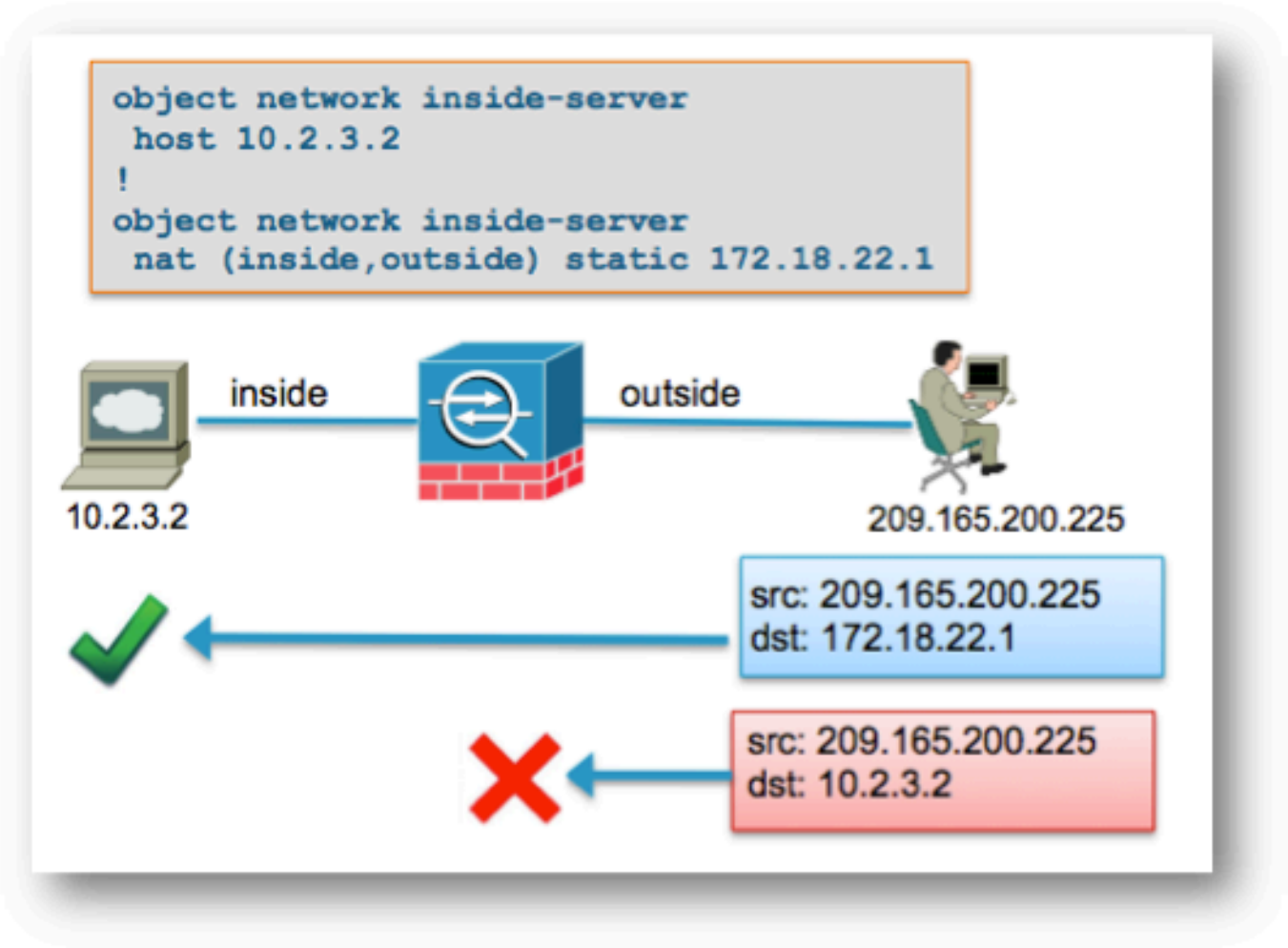
以下是在ASA上配置NAT時遇到的常見問題。

問題：由於NAT反向路徑故障(RPF)錯誤導致流量失敗：為轉發和反向流匹配的非對稱NAT規則

NAT RPF檢查可以確保ASA在轉發方向上轉換的連線(例如TCP同步(SYN))在反向方向上被同一NAT規則轉換，例如TCP SYN/確認(ACK)。

通常，此問題是由發往NAT語句中的本地（未轉換）地址的入站連線引起的。在基本級別，NAT RPF驗證從伺服器到客戶端的反向連線是否與同一NAT規則匹配；如果不匹配，則NAT RPF檢查失敗。

範例： 209.165.200.225



當位於192.168.200.225的外部主機將直接發往本地（未轉換）IP地址10.2.3.2的資料包時，ASA會丟棄該資料包並記錄此syslog：

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:192.168.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

解決方案：

首先，確保主機將資料傳送到正確的全局NAT地址。如果主機將資料包傳送到正確的地址，請檢查連線所命中的NAT規則。

驗證NAT規則是否定義正確，以及NAT規則中引用的對象是否正確。還要驗證NAT規則的順序是否合適。

使用Packet Tracer實用程式指定被拒絕資料包的詳細資訊。Packet tracer必須顯示由於RPF檢查失敗而丟棄的資料包。

接下來，檢視Packet Tracer的輸出，以檢視在NAT階段和NAT-RPF階段中遇到的NAT規則。

如果資料包與NAT RPF檢查階段中的NAT規則匹配（表示反向流將到達NAT轉換），但不與NAT階段中的規則匹配（表示正向流將不到達NAT規則），則丟棄該資料包。

此輸出與上圖所示的場景一致，即外部主機錯誤地將流量傳送到伺服器的本地IP地址而不是全局（轉換後的）IP地址：

```
<#root>

ASA#

packet-tracer input outside tcp 192.168.200.225 1234 10.2.3.2 80



    .....

Phase: 8
Type: NAT
Subtype: rpf-check
Result:

DROP


Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

如果資料包的目的地址是正確的對映IP地址172.18.22.1，則資料包會在向前方向的UN-NAT階段與正確的NAT規則匹配，並在NAT RPF-check階段與相同的規則匹配：

```
<#root>

ASA(config)#

packet-tracer input outside tcp 192.168.200.225 1234 172.18.22.1 80


...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
Subtype: rpf-check
Result:
```

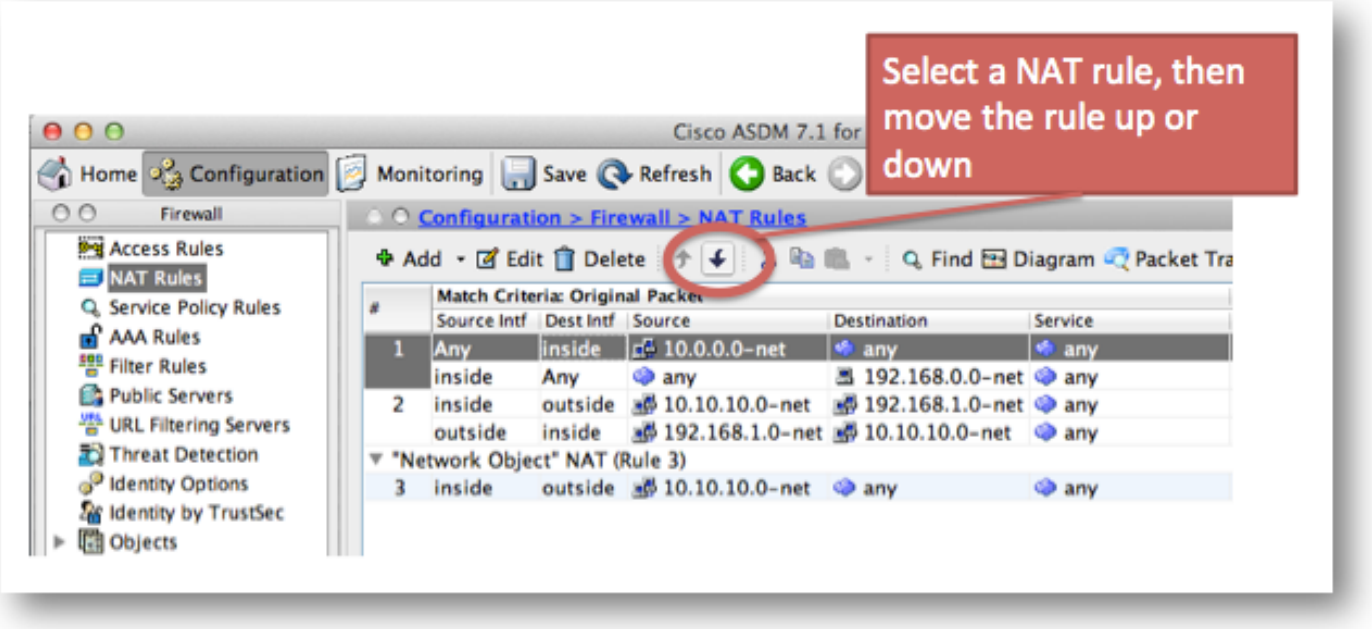
```
ALLOW

Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

問題：手動NAT規則順序混亂，導致不正確的資料包匹配

手動NAT規則根據它們在配置中的外觀進行處理。如果配置中首先列出一個非常廣泛的NAT規則，則它可以覆蓋NAT表中更下層的另一個更具體的規則。使用Packet Tracer驗證您的流量到達哪個NAT規則；可能需要將手動NAT條目重新排列到不同的順序。

解決方案：

使用ASDM重新排序NAT規則。



解決方案：

如果刪除規則並將其重新插入特定行號，則可以使用CLI對NAT規則進行重新排序。要在特定行插入新規則，請在指定介面後立即輸入行號。

範例：

```
<#root>

ASA(config)#

nat (inside,outside) 1 source static 10.10.10.0-net
10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net
```

問題

NAT規則過於寬泛，並且不慎與某些流量匹配。 有時會建立NAT規則，這些規則使用的對象過於廣泛。如果將這些規則放置在NAT表的頂部（例如，位於第1部分頂部），則它們可能比預期匹配的流量更多，並且會導致更靠下表的NAT規則永遠不會被命中。

解決方案

使用Packet Tracer確定您的流量是否與對象定義過於寬泛的規則匹配。如果是這種情況，您必須縮小這些對象的範圍，或者將規則進一步移到NAT表下方，或者移到NAT表的after-auto部分（第3部分）。

問題

NAT規則將流量轉移到不正確的介面。 當確定資料包從ASA傳出哪個介面時，NAT規則可以優先於路由表。如果入站資料包與NAT語句中轉換的IP地址匹配，則使用NAT規則來確定出口介面。

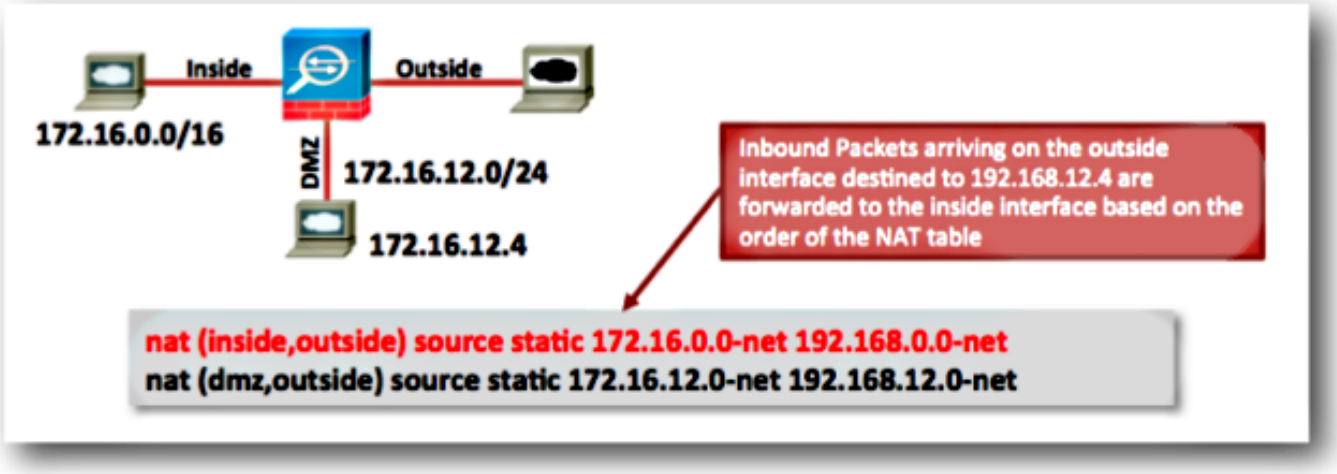
NAT轉移檢查（可覆蓋路由表）會檢查是否有任何NAT規則為到達介面的入站資料包指定目標地址轉換。

如果沒有規則明確指定如何轉換資料包目標IP地址，則會查詢全局路由表以確定出口介面。

如果有規則明確指定如何轉換資料包目標IP地址，則NAT規則會將資料包提取到轉換中的另一個介面，並有效地繞過全局路由表。

此問題最常見於入站流量（到達外部介面），並且通常是由將流量轉移到意外介面的NAT規則無序引起的。

範例：



解決方案：

此問題可透過以下任一操作解決：

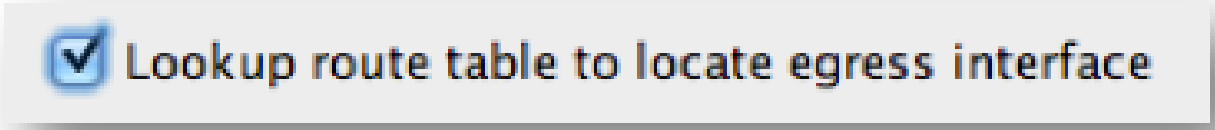
- 對NAT表重新排序，以便首先列出更具體的條目。
- 對NAT語句使用非重疊的全局IP地址範圍。

請注意，如果NAT規則是身份規則（這意味著規則不會更改IP地址），則可以使用route-lookup關鍵字（此關鍵字不適用於上一個示例，因為NAT規則不是身份規則）。

route-lookup關鍵字使ASA在匹配NAT規則時執行額外檢查。它檢查ASA的路由表是否將資料包轉發到此NAT配置將資料包轉發到的同一輸出介面。

如果路由表出口介面與NAT轉移介面不匹配，則NAT規則不匹配（跳過該規則），資料包繼續沿著NAT表向下移動，以由後來的NAT規則進行處理。

route-lookup選項僅在NAT規則是身份NAT規則時可用，這意味著規則不會更改IP地址。如果將路由查詢增加到NAT行的末尾，或者在ASDM中的NAT規則配置中選中Lookup route table to locate egress interface覈取方塊，則可以對NAT規則啟用route-lookup選項：



問題：NAT規則導致ASA為對映介面上的流量代理地址解析協定(ARP)

ASA代理ARP在全局介面的NAT語句中為全局IP地址範圍提供ARP。如果向NAT語句增加no-proxy-arp關鍵字，則可以根據每個NAT規則停用此代理ARP功能。

如果無意中建立了全局地址子網，而該子網比原來想要的要大得多，也會出現此問題。

解決方案

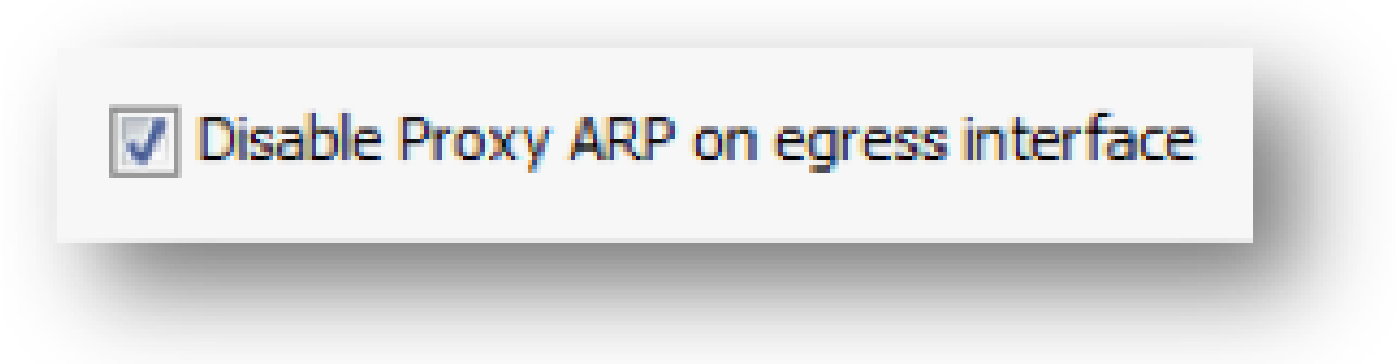
如果可能，將no-proxy-arp關鍵字增加到NAT行。

範例：

```
<#root>

ASA(config)#

object network inside-server

ASA(config-network-object)#

nat (inside,outside) static 172.18.22.1 no-proxy-arp

ASA(config-network-object)#

end
```

```
ASA#
  ASA#

 show run nat


object network inside-server
 nat (inside,outside) static 172.18.22.1

no-proxy-arp


ASA#
```

這也可以透過ASDM來實現。在NAT規則中，選中Disable Proxy ARP on egress interface覈取方塊。



.

相關資訊

- 影片：DMZ伺服器訪問的ASA埠轉發（版本8.3和8.4）
- 基本ASA NAT配置：ASA版本8.3及更高版本中DMZ中的Web伺服器
- 書冊2：Cisco ASA系列防火牆CLI配置指南，9.1
- 思科技術支援與下載

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）。