ASA上的DNS修正配置示例

目錄

簡介

本文檔介紹如何在自適應安全裝置(ASA)上使用DNS修正來更改域名系統(DNS)響應中的嵌入式IP地址，以便客戶端可以連線到伺服器的正確IP地址。

必要條件

需求

DNS修正要求在ASA上配置網路地址轉換(NAT)並啟用DNS檢查。

採用元件

本文檔中的資訊基於自適應安全裝置。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

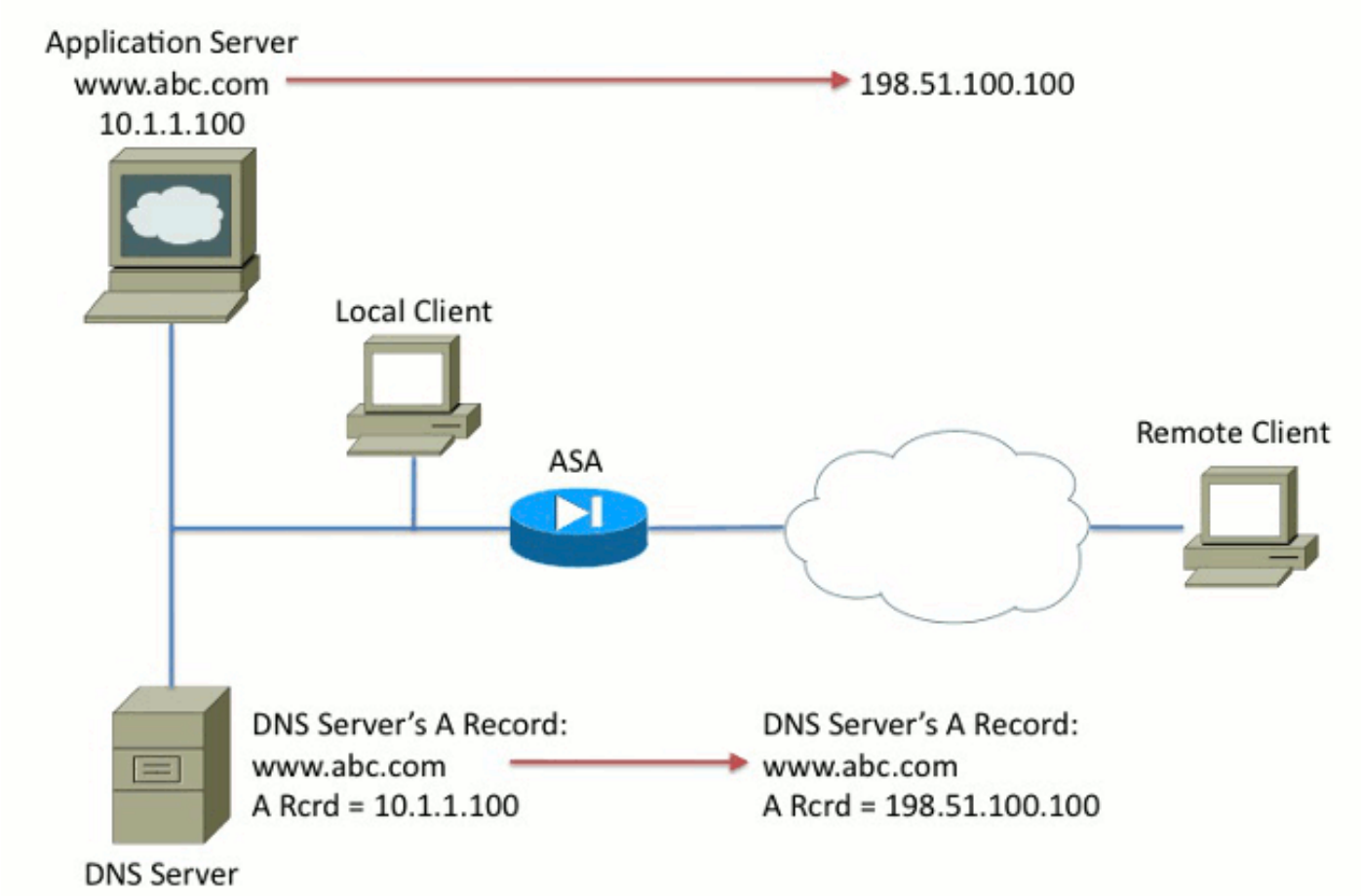
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

DNS修正示例

ASA內部的DNS伺服器

圖1



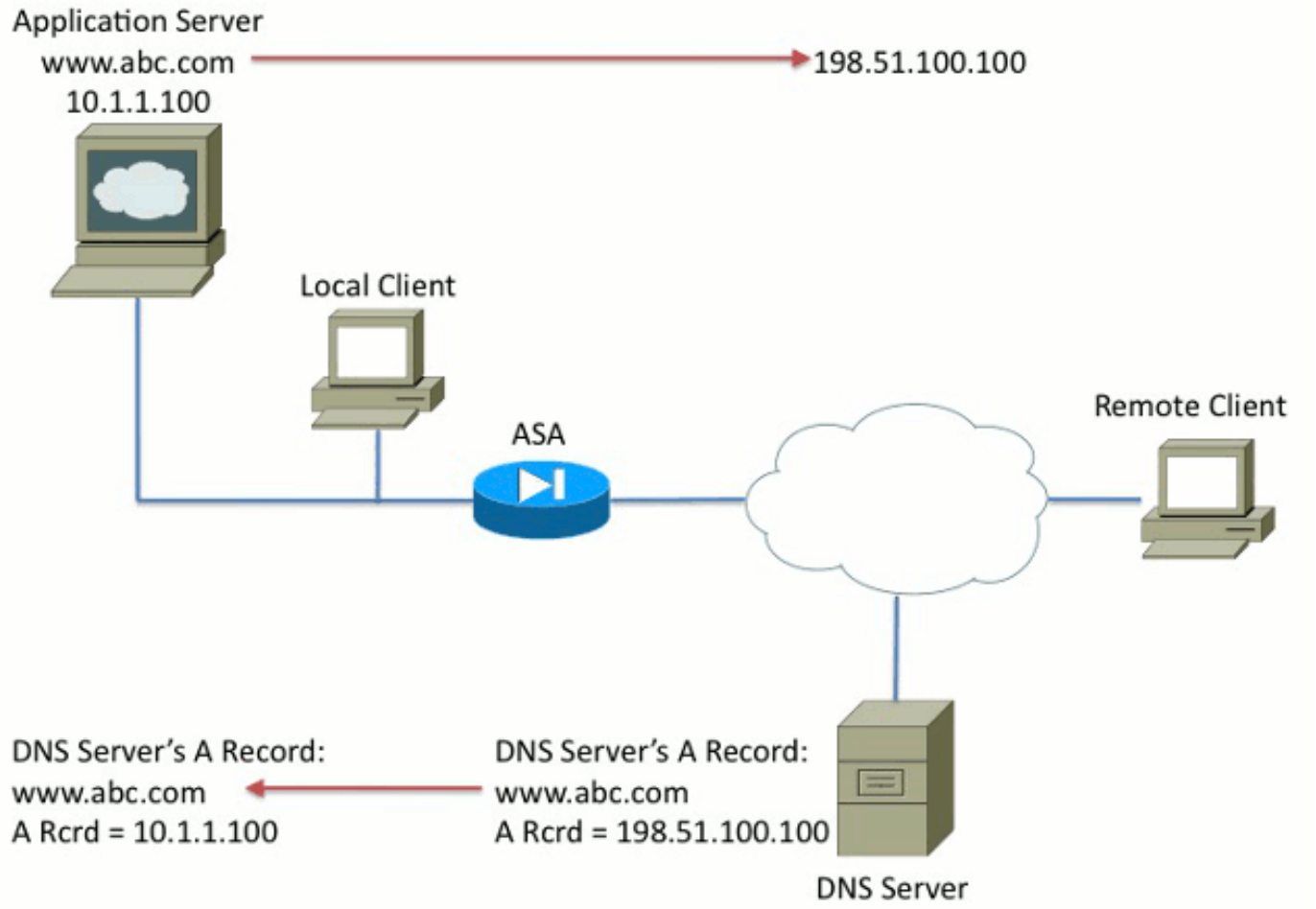

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

在圖1中，DNS伺服器由本地管理員控制。DNS伺服器應分發一個私有IP地址，即分配給應用伺服器的實際IP地址。這允許本地客戶端直接連線到應用伺服器。

很遺憾，遠端客戶端無法使用私有地址訪問應用伺服器。因此，在ASA上配置了DNS修正以更改DNS響應資料包中的嵌入式IP地址。這可確保當遠端客戶端對www.abc.com發出DNS請求時，它們獲得的響應是針對應用伺服器的轉換地址。如果沒有NAT語句中的DNS關鍵字，遠端客戶端會嘗試連線到10.1.1.100，但該地址無法在Internet上路由，因此不起作用。

ASA外部的DNS伺服器

圖2



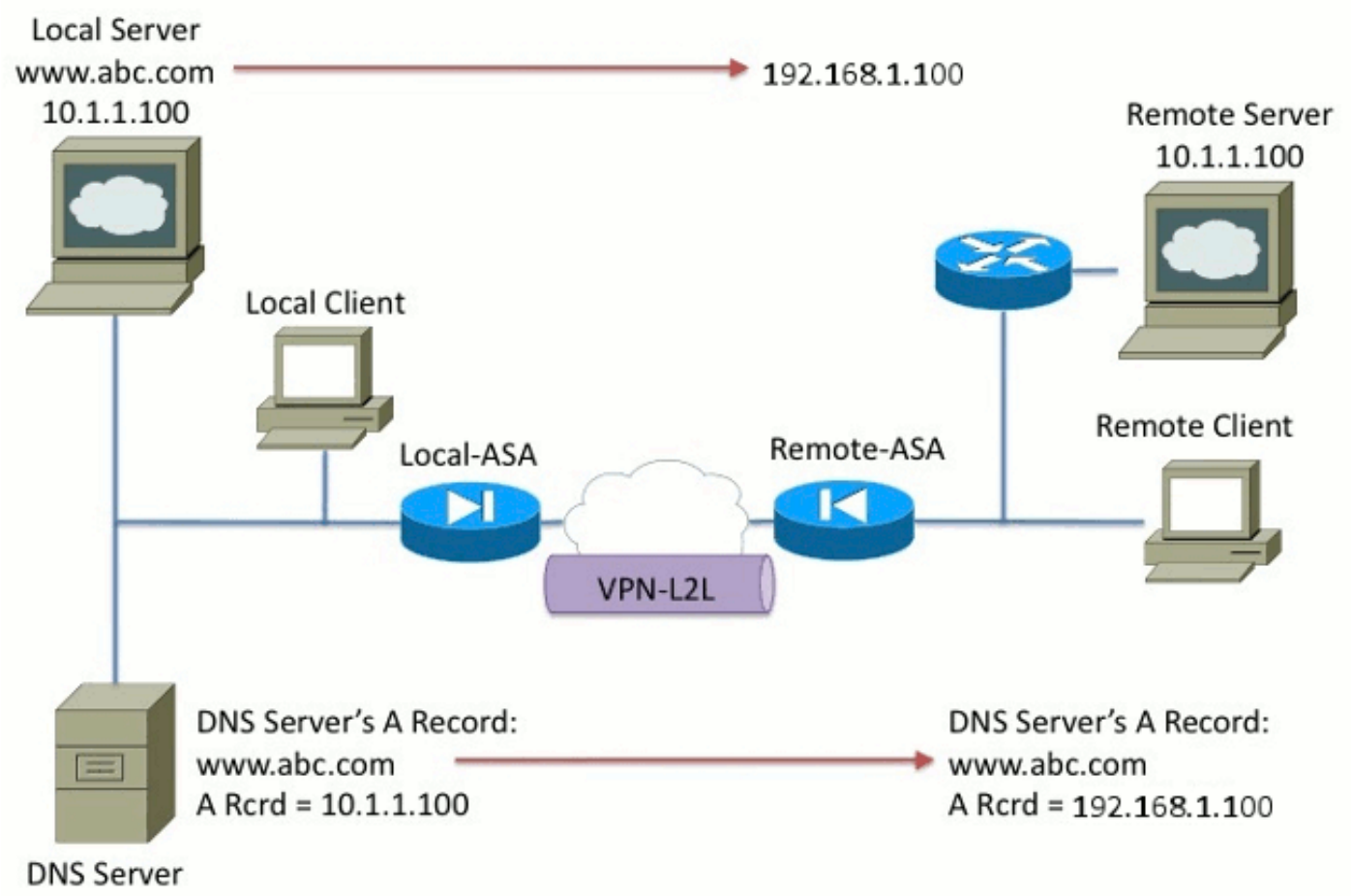

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

在圖2中，DNS伺服器由ISP或類似服務提供商控制。DNS伺服器應分發公共IP地址，即應用伺服器的轉換的IP地址。這允許所有Internet使用者通過Internet訪問應用伺服器。

很遺憾，本地客戶端無法使用公共地址訪問應用伺服器。因此，在ASA上配置了DNS修正以更改DNS響應資料包中的嵌入式IP地址。這可確保當本地客戶端對www.abc.com發出DNS請求時，收到的響應是應用伺服器的實際地址。如果沒有NAT語句上的DNS關鍵字，本地客戶端會嘗試連線到198.51.100.100。該操作不起作用，因為此資料包被傳送到ASA，ASA丟棄該資料包。

VPN NAT和DNS修正

圖3



請考慮網路重疊的情況。在這種情況下，地址10.1.1.100同時位於遠端端和本地端。因此，您需要在本地伺服器上執行NAT，以便遠端客戶端仍然可以使用IP地址192.1.1.100訪問它。為了使其正常工作，需要DNS修正。

無法在此函式中執行DNS修正。只能將DNS關鍵字新增到對象NAT或源NAT的末尾。兩次NAT不支援DNS關鍵字。有兩種可能配置，但都失敗。

失敗的配置1：如果配置底線，它將10.1.1.1轉換為192.1.1.1，不僅適用於遠端客戶端，而且適用於Internet上的每個使用者。由於192.1.1.1不是Internet可路由的，因此Internet上的任何人都無法訪問本地伺服器。

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
```

失敗配置2:如果在必要的兩次NAT線路後配置DNS修正NAT線路，則會導致DNS修正永遠無法正常運行的情況。因此，遠端使用者端嘗試存取IP位址為10.1.1.100的www.abc.com，但無法使用。

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- Cisco ASA 5500系列自適應安全裝置>軟體下載
- 技術支援與文件 - Cisco Systems

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）。