如何配置IP欺騙？

目錄

問題

如何配置IP欺騙？

環境:思科網路安全裝置(WSA),AsyncOS的所有版本

摘要:

在傳統的代理部署中，客戶端的IP地址被替換為代理/快取伺服器的IP地址。雖然這樣通過遮蔽終端使用者的地址提供了固有的安全性，但在某些情況下，某些Web應用程式需要訪問始發客戶端的IP地址。

通過在Cisco Web Security Appliance(WSA)中實施「IP欺騙」功能並在Cisco IOS裝置上配置適當的WCCP服務組，可以將客戶端的IP地址呈現給Web應用，而不是WSA的IP地址。以下文檔介紹了此實施所需的配置步驟。

說明:

要實施「IP欺騙」功能，需要在Cisco IOS®路由器上建立兩個唯一的WCCP服務組。第一個WCCP「web-cache」組將來自使用者的http/埠80流量重定向到WSA。可以配置特定訪問控制清單（如下例所示），以控制哪些使用者受思科網路安全裝置保護。路由器上的使用者介面配置為將入站流量重定向到此WCCP服務組。

第二個WCCP服務組需要定義為動態服務ID（例如服務ID 95）。 同樣，訪問清單用於控制哪些使用者受到保護（即允許完全繞過系統）。 對於返回的Web流量，路由器上的外部介面配置為將其入站流量重定向到WCCP服務組95。