

# How do I configure IP spoofing?



Document ID: 117949

Contributed by Cordelia Naumann and Siddharth Rajpathak, Cisco TAC Engineers.

Jul 16, 2014

## Contents

### Question

## Question

How do I configure IP spoofing?

Environment: Cisco Web Security Appliance (WSA), all versions of AsyncOS

### *Abstract:*

In a traditional proxy deployment the client's IP address is replaced with that of the proxy/cache server. While this provides inherent security by masking the address of the end user, in some cases certain web applications require access to the originating client's IP address.

By implementing the "IP Spoofing" feature in the Cisco Web Security Appliance (WSA) and configuring the appropriate WCCP service groups on a Cisco IOS device, it is possible to present the client's IP address to web applications instead of WSA's IP address. The following document describes the necessary configuration steps for this implementation.

### *Description:*

To implement the "IP Spoofing" feature, two unique WCCP service groups needed to be created on a Cisco IOS® router. The first WCCP 'web-cache' group redirects http/port 80 traffic from the user to the WSA. Specific access control lists can be configured (as shown in the example below) to control which users are protected by the Cisco Web Security appliance. The user interface on the router is configured to redirect inbound traffic to this WCCP service group.

The second WCCP service group needs to be defined as a dynamic service ID (say service ID 95). Again an access list is used to control what users are protected (i.e. allow for bypassing of the system altogether). For the return web traffic, the outside interface on the router is configured to redirect its inbound traffic to the WCCP service group 95.