How to Configure IP Spoofing aka Reflect IP on Cisco Secure Web Appliance in AsyncOS 12.5

Introduction

In AsyncOS 12.5, we have introduced an extension to the basic IP spoofing functionality. This feature allows us to configure IP spoofing to point a specific URL category to a different IP address. However, this feature is not available for Native FTP connections.

Policy Trace

Using connection tracing, the connectivity to the origin server can be verified using the spoofed IP address. The Policy Trace tool is available via System Administration -> Policy Trace. This tool is enhanced to perform connection tracing.

Access Logs

Access logs for client spoofing for native FTP are moved to the Policy Trace feature. The new formatter option allows showing the spoofed IP address. It can be used with the access log keyword. The access log can be displayed in the CLI as well.

Routing Policies

Routing policies will have one additional section to configure IP spoofing. Unlike global IP spoofing, proxy IP spoofing will be configured in routing policies. The routing policy will determine which IP address will be used as the source IP. When a response (traffic) will land on the Secure Web Appliance instead of the client, additional provisioning on the WCCP router is required so incoming web traffic will be sent as the source IP. But when IP spoofing is enabled, the client's original IP (Secure Web Appliance visible client IP) is used as the source IP.

IP Spoofing Profiles

For achieving the above requirements, IP spoofing profiles are introduced. These profiles can be used to configure IP spoofing based on the predefined URL category or custom category. The profiles can be created under Web Security Manager -> IP Spoofing Profiles.

Feature Configuration

In RockyOS 12.5, we have added support for IP spoofing profiles. HTTPS decryption is required for YouTube traffic to retrieve the token ID from the URL.

File and Directory Transfers

IP spoofing connection type for file and directory transfers can be added on the Secure Web Appliance. IP spoofing connection type applies to only explicit connections if the proxy mode is configured as Forward.

Solution Path

1. Proxy Mode: Transparent – allows both transparent and explicitly redirected requests from the clients.
2. Solution path: In this case, it seems the customer requires a different upstream security stack to be applied for each of the branches.
3. "Government services use source-based routing to send requests for specific TLDs (".com" vs. ".mil" vs. ".gov") to different web servers."
4. Solution path: In this case, it seems the customer requires a different upstream security stack to be applied for each of the branches.
5. IP spoofing will typically benefit organizations that have geopolitical requirements or software-as-a-service (SaaS) applications.
6. IP spoofing can also assist with segregating different application data on your network based on subnets, ports, protocols, URL categories, and more.