Configuring IP Spoofing

Cisco ISR and IronPort Web Security Appliance

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 clients IP address.

By implementing the “IP Spoofing” feature in the IronPort 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 that of the WSA. 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 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 IronPort 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 “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.
Equipment:

Cisco ISR Router
Tested w/ 12.4(15)T – Advanced Enterprise

Note: There is nothing specific to the IOS release tested – should work on any router that supports WCCPv2

IronPort S-650
Tested w/ 5.2.0-428

Configuration:

Router –

ip wccp web-cache redirect-list redirect-list group-list group-list password cisco
ip wccp 95 redirect-list redirect-return group-list group-list password cisco

interface GigabitEthernet0/0
description Trunk
no ip address
duplex auto
speed auto

interface GigabitEthernet0/0.10
description Outbound Interface
encapsulation dot1Q 10
ip address 10.10.42.2 255.255.255.0
ip wccp 95 redirect in
!
interface GigabitEthernet0/0.65
description Cache Network
encapsulation dot1Q 65
ip address 10.10.10.2 255.255.255.0
!
interface GigabitEthernet0/0.99
description User Network
encapsulation dot1Q 99
ip address 192.168.99.2 255.255.255.0
ip wccp web-cache redirect in
!
ip access-list standard group-list
permit 10.10.10.65
!
ip access-list extended redirect-list
permit tcp 192.168.99.0 0.0.0.255 any eq www

ip access-list extended redirect-return
permit tcp any eq www 192.168.99.0 0.0.0.255
IronPort

WCCP Service for outbound traffic

WCCP Service for return traffic
Enable IP Spoofing

Edit Web Proxy Settings

<table>
<thead>
<tr>
<th>Web Proxy Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Proxy</td>
<td>On (default)</td>
</tr>
<tr>
<td>Ports to Proxy</td>
<td>80, 8080</td>
</tr>
<tr>
<td>Cache</td>
<td>ON (default)</td>
</tr>
<tr>
<td>IP Spoofing</td>
<td>Enable (default)</td>
</tr>
<tr>
<td>When enabling IP spoofing, if using a WCCP router, ensure that Service ID 98 is used.</td>
<td></td>
</tr>
</tbody>
</table>

**Advanced Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserve Timeout</td>
<td>500 seconds</td>
</tr>
<tr>
<td>Persistent Timeout</td>
<td>500 seconds</td>
</tr>
<tr>
<td>Simultaneous Persistent Connections</td>
<td>64</td>
</tr>
<tr>
<td>Server Maximum Number</td>
<td>2000</td>
</tr>
</tbody>
</table>

**Headers**

- **X-Forwarded-For**
  - Send (default)
  - Do Not Send
- **Via**
  - Send (default)
  - Do Not Send