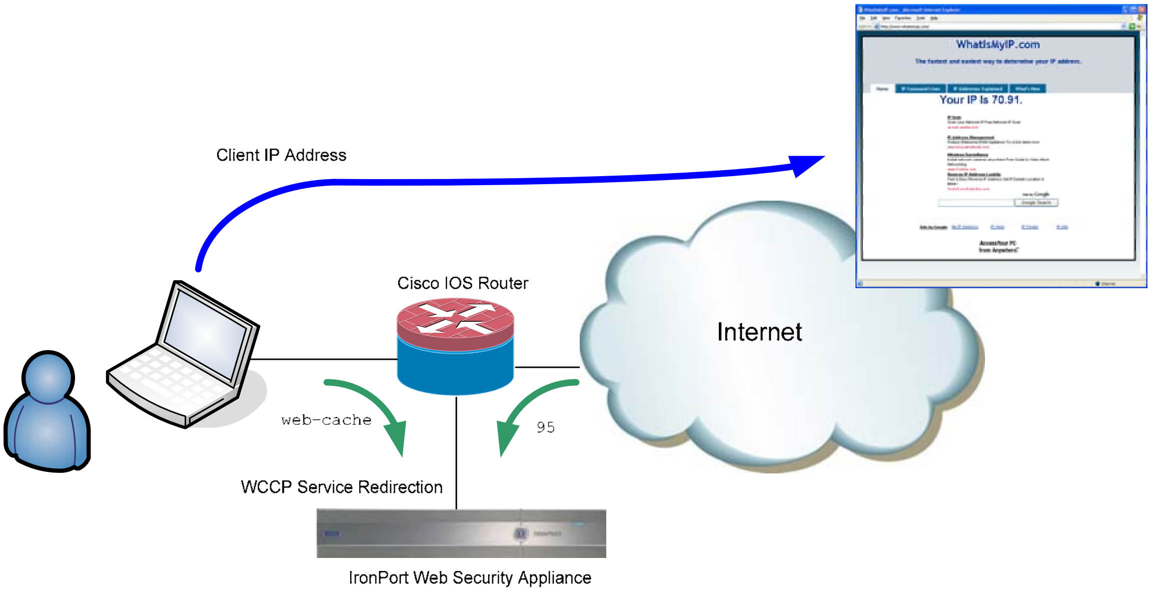
Configuring IP Spoofing

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 would on any router that supports
WCCPv2
```

IronPort S-650

Tested w/ 5.2.0-428

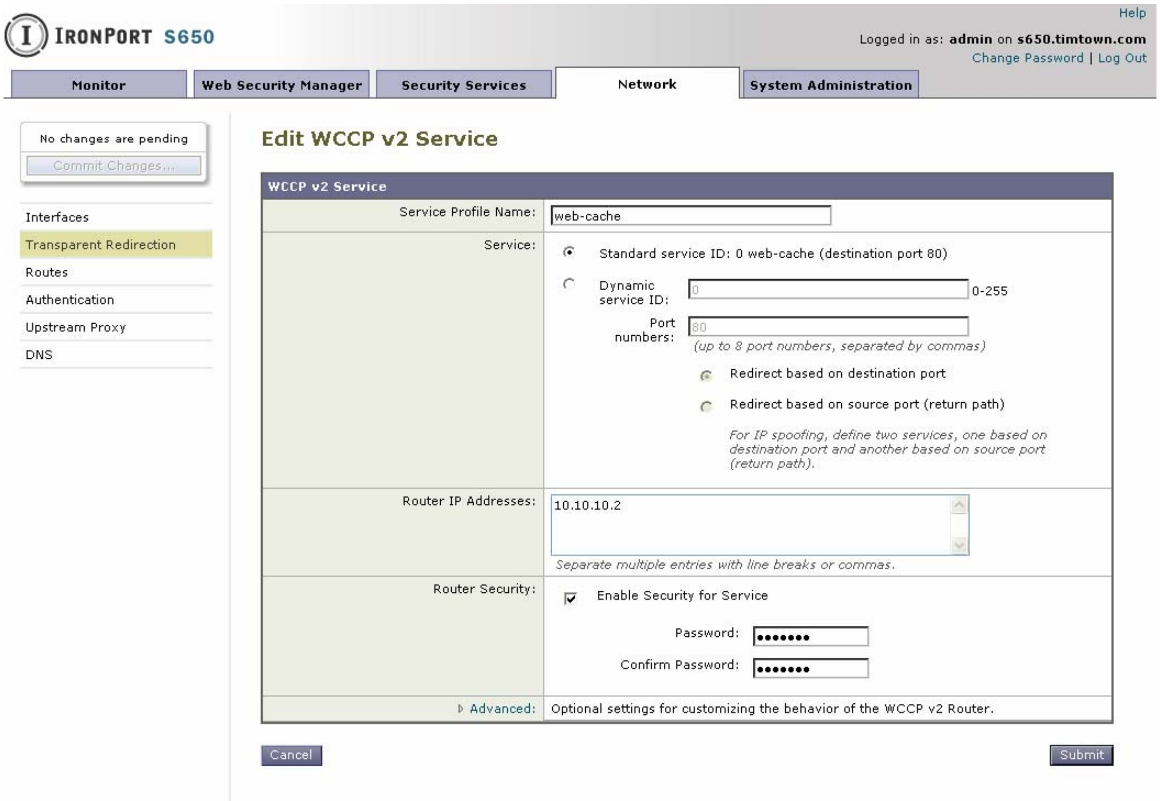
Configuration:

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



Edit WCCP v2 Service

WCCP v2 Service

Service Profile Name: web-cache

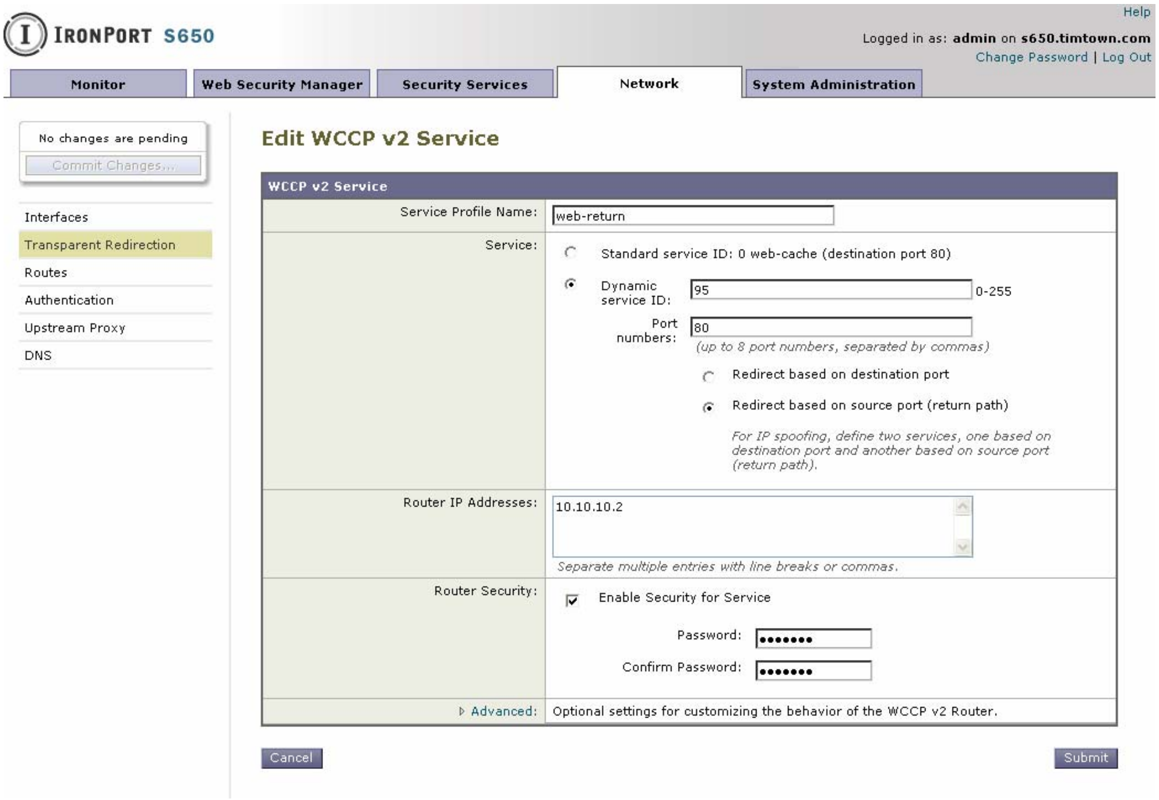
Service:
● Standard service ID: 0 web-cache (destination port 80)
○ Dynamic service ID: 0 0-255
Port numbers: 80 (up to 8 port numbers, separated by commas)
● Redirect based on destination port
○ Redirect based on source port (return path)
For IP spoofing, define two services, one based on destination port and another based on source port (return path).

Router IP Addresses: 10.10.10.2
Separate multiple entries with line breaks or commas.

Router Security: ☑ Enable Security for Service
Password: •••••••
Confirm Password: •••••••

▹ Advanced: Optional settings for customizing the behavior of the WCCP v2 Router.

WCCP Service for return traffic



Edit WCCP v2 Service

WCCP v2 Service

Service Profile Name: web-return

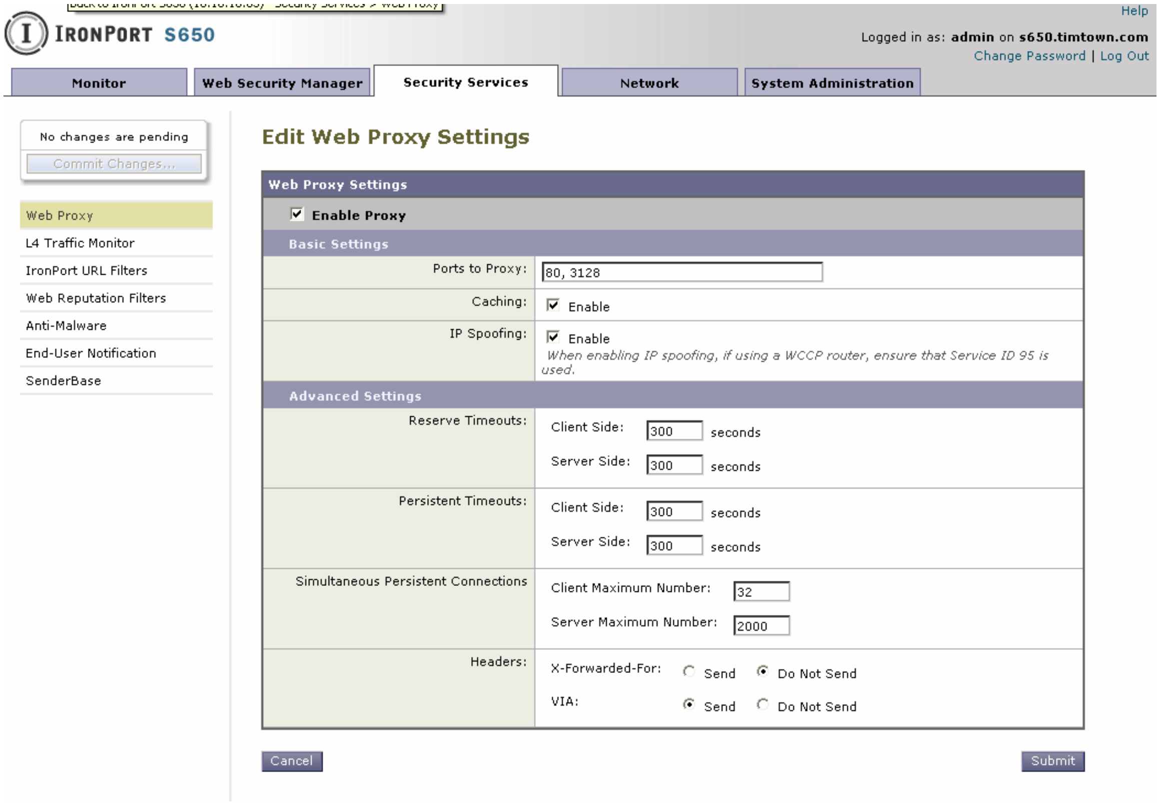
Service:
○ Standard service ID: 0 web-cache (destination port 80)
● Dynamic service ID: 95 0-255
Port numbers: 80 (up to 8 port numbers, separated by commas)
○ Redirect based on destination port
● Redirect based on source port (return path)
For IP spoofing, define two services, one based on destination port and another based on source port (return path).

Router IP Addresses: 10.10.10.2
Separate multiple entries with line breaks or commas.

Router Security: ☑ Enable Security for Service
Password: •••••••
Confirm Password: •••••••

▹ Advanced: Optional settings for customizing the behavior of the WCCP v2 Router.

Enable IP Spoofing



Logged in as: **admin** on **s650.timtown.com**
Change Password | Log Out

No changes are pending

Edit Web Proxy Settings

Web Proxy Settings

☑ **Enable Proxy**

Basic Settings

Ports to Proxy:	80, 3128
Caching:	☑ Enable
IP Spoofing:	☑ Enable *When enabling IP spoofing, if using a WCCP router, ensure that Service ID 95 is used.*

Advanced Settings

Reserve Timeouts:	Client Side: 300 seconds Server Side: 300 seconds
Persistent Timeouts:	Client Side: 300 seconds Server Side: 300 seconds
Simultaneous Persistent Connections	Client Maximum Number: 32 Server Maximum Number: 2000
Headers:	X-Forwarded-For: ○ Send ● Do Not Send VIA: ● Send ○ Do Not Send