

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[WSA Configuration](#)

[Sample ASA Configuration](#)

[Sample Switch Configuration \(c3560\)](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure the Web Security Appliance (WSA) / Cisco Router in order to support transparent redirection of HTTP, HTTPS, and Native FTP traffic with Web Cache Communication Protocol (WCCP).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Web Security Appliance that runs AsyncOS Version 6.0 or later
- Native FTP proxy enabled on WSA
- WCCPv2 compatible Cisco Router/Switch or ASA Firewall

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

When Native FTP traffic is redirected transparently to the WSA, the WSA typically receives the traffic on the standard FTP port 21. Hence, the Native FTP proxy on the WSA should listen on port 21 (by default the native FTP proxy is 8021). In the GUI, choose **Security Services > FTP Proxy** for verification.

WSA Configuration

1. Create an identity for FTP traffic. In the GUI, choose **Web Security Manager > Identities** and ensure that authentication has been disabled for this ID.
2. Create an access policy. In the GUI, choose **Web Security Manager > Access Policies**, which references the identity in step 1.
3. Under FTP proxy settings, modify the FTP Passive ports to be 11000-11006 in order to ensure that all ports fit into a single service group.
4. Create these WCCP Service IDs:

<u>Name</u>	<u>Service</u>	<u>Ports</u>
web-cache	0	80 (<i>alternatively, you can use 98 custom-web-cache if you use multiple WSAs</i>)
ftp-native	60	21,11000,11001,11002,11003,11004,11005,11006
https-cache	70	443

These examples redirect three internal subnets while they bypass WCCP redirection for all privately addressed destinations as well as a single internal host.

Sample ASA Configuration

```
wccp web-cache redirect-list web-cache group-list group_acl
wccp 60 redirect-list ftp-native group-list group_acl
wccp 70 redirect-list https-cache group-list group_acl

wccp interface inside web-cache redirect in
wccp interface inside 60 redirect in
wccp interface inside 70 redirect in

access-list group_acl extended permit ip host 10.1.1.160 any

access-list ftp-native extended deny ip any 10.0.0.0 255.0.0.0
access-list ftp-native extended deny ip any 172.16.0.0 255.240.0.0
access-list ftp-native extended deny ip any 192.168.0.0 255.255.0.0
access-list ftp-native extended deny ip host 192.168.42.120 any
access-list ftp-native extended permit tcp 192.168.42.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.42.0 255.255.255.0 any range 11000
11006
access-list ftp-native extended permit tcp 192.168.99.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.99.0 255.255.255.0 any range 11000
11006
access-list ftp-native extended permit tcp 192.168.100.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.100.0 255.255.255.0 any range 11000
11006

access-list https-cache extended deny ip any 10.0.0.0 255.0.0.0
access-list https-cache extended deny ip any 172.16.0.0 255.240.0.0
access-list https-cache extended deny ip any 192.168.0.0 255.255.0.0
access-list https-cache extended deny ip host 192.168.42.120 any
access-list https-cache extended permit tcp 192.168.42.0 255.255.255.0 any eq https
access-list https-cache extended permit tcp 192.168.99.0 255.255.255.0 any eq https
access-list https-cache extended permit tcp 192.168.100.0 255.255.255.0 any eq https

access-list web-cache extended deny ip any 10.0.0.0 255.0.0.0
access-list web-cache extended deny ip any 172.16.0.0 255.240.0.0
access-list web-cache extended deny ip any 192.168.0.0 255.255.0.0
access-list web-cache extended deny ip host 192.168.42.120 any
access-list web-cache extended permit tcp 192.168.42.0 255.255.255.0 any eq www
access-list web-cache extended permit tcp 192.168.99.0 255.255.255.0 any eq www
access-list web-cache extended permit tcp 192.168.100.0 255.255.255.0 any eq www
```

Sample Switch Configuration (c3560)

This should work on most routers too.

```
ip wccp web-cache redirect-list web-cache group-list group_acl
ip wccp 60 redirect-list ftp-native group-list group_acl
ip wccp 70 redirect-list https-cache group-list group_acl
```

```
interface Vlan99
ip address 192.168.99.1 255.255.255.0
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in
```

```
interface Vlan100
ip address 192.168.100.1 255.255.255.0
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in
```

```
interface Vlan420
ip address 192.168.42.1 255.255.255.0
ip helper-address 192.168.100.20
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in
```

```
ip access-list extended ftp-native
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq ftp
permit tcp 192.168.42.0 0.0.0.255 any range 11000 11006
permit tcp 192.168.99.0 0.0.0.255 any eq ftp
permit tcp 192.168.99.0 0.0.0.255 any range 11000 11006
permit tcp 192.168.100.0 0.0.0.255 any eq ftp
permit tcp 192.168.100.0 0.0.0.255 any range 11000 11006
```

```
ip access-list extended https-cache
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq 443
permit tcp 192.168.99.0 0.0.0.255 any eq 443
permit tcp 192.168.100.0 0.0.0.255 any eq 443
```

```
ip access-list extended web-cache
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq www
permit tcp 192.168.99.0 0.0.0.255 any eq www
permit tcp 192.168.100.0 0.0.0.255 any eq www
```

```
ip access-list standard group_acl
permit 10.1.1.160
```

Note: Due to a WCCP technology limitation, a maximum of eight ports can be assigned per WCCP service ID.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.