

**FORTINET**

*an excerpt from*  
✓

# The FortiGate™ Cookbook

FortiOS 4.0 MR3

Extending AirPlay and AirPrint communication  
through a FortiWiFi unit



Fortinet Publishing

# Extending AirPlay and AirPrint communication through a FortiWiFi unit

## Problem

How do I use AirPlay and Air print when a FortiWiFi unit separates client and server AirPlay and AirPrint devices.

## Solution

To configure the FortiWiFi unit to allow printing to an AirPrint-compatible printer, the network topology determines the solution. For example, if an iPhone and an AirPrint-compatible printer both use WiFi to connect to the same FortiWiFi wireless access point on the same subnet, no FortiWiFi configuration changes are required as long as intra-SSID traffic is not blocked. The iPhone and the printer can communicate directly.

If the iPhone and the AirPrint-compatible printer are on different networks separated by a FortiWiFi unit you can use the information below to set all AirPrint communication through the FortiWiFi unit.

The following examples also describe how to allow AirPlay communication between AirPlay devices also separated by a FortiWiFi unit.

### Enable multicast forwarding

If you require AirPrint or AirPlay traffic to pass through a FortiWiFi unit, the first step is to enable multicast forwarding in the FortiWiFi unit.

- 1 Enter the following CLI command to enable multicast forwarding:

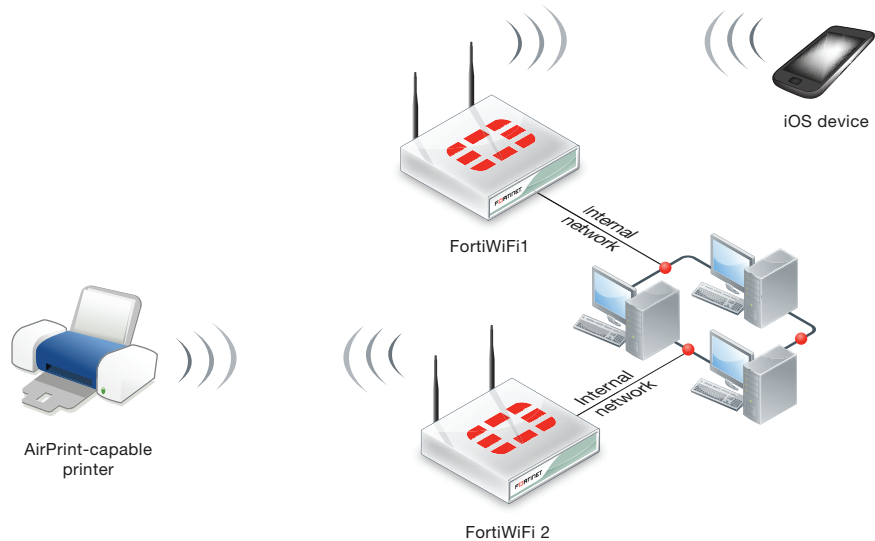
```
config system settings
  set multicase-forward enable
end
```

- 2 Create multicast security policies to allow the multicast traffic to pass.

```
config firewall multicast-policy
  edit 1
    set dstaddr 224.0.0.251 255.255.255.255
    set dstintf "port2"
    set srcintf "port1"
    set protocol 17
    set end-port 5353
    set action accept
  next
  edit 2
    set dstaddr 224.0.0.251 255.255.255.255
    set dstintf "port1"
    set srcintf "port2"
    set protocol 17
    set end-port 5353
    set action accept
  next
end
```

## AirPrint from iOS

To allow an iOS device (iPhone, iPad, or iPod Touch) to print to an AirPrint enabled printer on separate WiFi networks, configure the FortiWiFi units according to these procedures:



- 1 On both FortiWiFi units, enable multicast forwarding and create security policies to allow multicast traffic. See “[Enable multicast forwarding](#)” on page 2.
- 2 Go to **Firewall Objects > Service > Custom** and select **Create New** to create an Internet Printing Protocol (IPP) custom service for AirPrint:

<b>Name</b>	IPP
<b>Protocol Type</b>	TCP/UDP/SCTP
<b>Protocol</b>	TCP
<b>Source Port Low</b>	1
<b>Source Port High</b>	65535
<b>Destination Port Low</b>	631
<b>Destination Port High</b>	631

- 3 Select **OK**.

- 4 On FortiWiFi 1 go to **Policy > Policy > Policy** and select **Create New** to add a security policy to allow the AirPrint traffic from the wireless network to the internal network.

<b>Source Interface/Zone</b>	wlan
<b>Source Address</b>	all
<b>Destination Interface/Zone</b>	internal
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	IPP
<b>Action</b>	ACCEPT

- 5 Select **OK**.
- 6 On FortiWiFi 2 go to **Policy > Policy > Policy** and select **Create New** to add a security policy to allow the AirPrint traffic from the internal network to the wireless network.

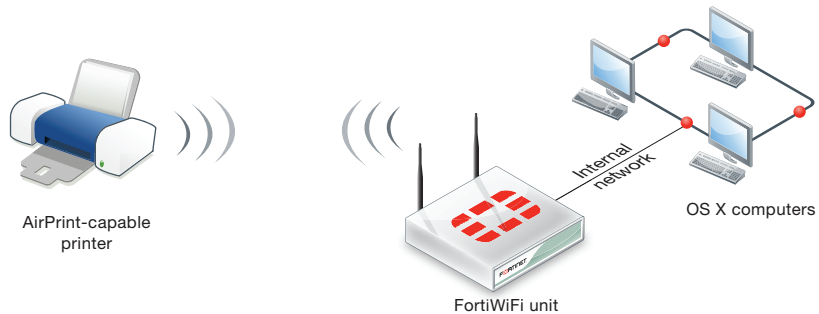
<b>Source Interface/Zone</b>	internal
<b>Source Address</b>	all
<b>Destination Interface/Zone</b>	wlan
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	IPP
<b>Action</b>	ACCEPT

- 7 Select **OK**.

With this configuration in place, anyone using an iOS device on FortiWiFi 1's wireless network can use AirPrint to print to the printer.

## AirPrint from OS X

To allow an OS X computer to print to an AirPrint enabled printer on a WiFi network, configure the FortiWiFi unit according to these procedures:



- 1 Enable multicast forwarding and create security policies to allow multicast traffic. See [“Enable multicast forwarding” on page 2](#).
- 2 Go to **Firewall Objects > Service > Custom** and select **Create New** to create a PDL data streaming custom service:

<b>Name</b>	PDL
<b>Protocol Type</b>	TCP/UDP/SCTP
<b>Protocol</b>	TCP
<b>Source Port Low</b>	1
<b>Source Port High</b>	65535
<b>Destination Port Low</b>	9100
<b>Destination Port High</b>	9100

- 3 Select **OK**.
- 4 Select **Create New** to allow AirPrint traffic from the internal network to the wireless network:

<b>Source Interface/Zone</b>	internal
<b>Source Address</b>	all

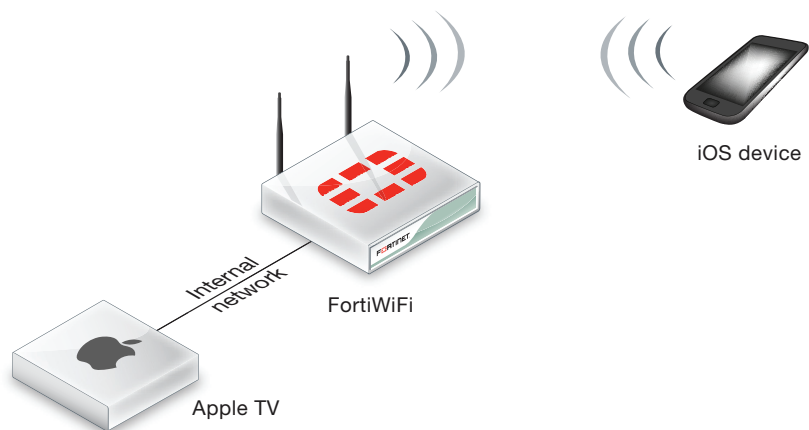
<b>Destination Interface/Zone</b>	wlan
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	IPP
<b>Action</b>	ACCEPT

5 Select **OK**.

With this configuration in place, anyone using an OS X computer on the network connected to the internal interface of the FortiWiFi unit can use AirPrint to print to the printer.

### AirPlay from iOS

To allow an iOS device (iPhone, iPad, or iPod Touch) to play to an Apple TV on a separate network, configure the FortiWiFi unit according to these procedures:



- 1 Enable multicast forwarding and create security policies to allow multicast traffic. See ["Enable multicast forwarding"](#) on page 2.

- Go to **Firewall Objects > Service > Custom** and select **Create New** to create a new custom service with these characteristics:

<b>Name</b>		AirPlay - iOS to Apple TV		
<b>Protocol Type</b>		TCP/UDP/SCTP		
<b>Protocol</b>	<b>Source Port Low</b>	<b>Source Port High</b>	<b>Destination Port Low</b>	<b>Destination Port High</b>
TCP	1	65535	7000	7000
TCP	1	65535	7100	7100
TCP	1	65535	49152	50000
UDP	1	65535	1	65535

- Select **OK**.
- Select **Create New** to create another new custom service with these characteristics:

<b>Name</b>		AirPlay - Apple TV to iOS		
<b>Protocol Type</b>		TCP/UDP/SCTP		
<b>Protocol</b>	<b>Source Port Low</b>	<b>Source Port High</b>	<b>Destination Port Low</b>	<b>Destination Port High</b>
TCP	1	65535	7000	7000
UDP	1	65535	1	65535

- Select **OK**.
- Go to **Policy > Policy > Policy** and select **Create New** to create a security policy to allow AirPlay traffic from the wireless network to the internal network.

<b>Source Interface/Zone</b>	wlan
<b>Source Address</b>	all

<b>Destination Interface/Zone</b>	internal
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	AirPlay - iOS to Apple TV
<b>Action</b>	ACCEPT

- 7 Select **OK**.
- 8 Select **Create New** to create a security policy to allow the AirPlay traffic from the internal network to the wireless network.

<b>Source Interface/Zone</b>	internal
<b>Source Address</b>	all
<b>Destination Interface/Zone</b>	wlan
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	AirPlay - Apple TV to iOS
<b>Action</b>	ACCEPT

- 9 Select **OK**.

With this configuration in place, anyone using an iOS device on the wireless interface of the FortiWiFi unit can use AirPlay to play media on the Apple TV.

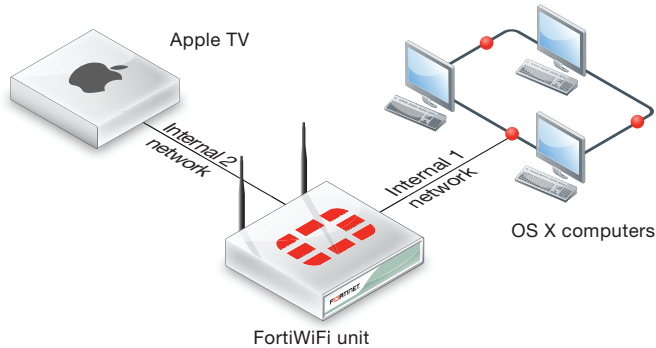


Although AirPlay will function with this configuration, playing You Tube video requires that security policies allow the iOS device and the Apple TV to access the Internet.



### AirPlay from OS X

To allow an OS X computer to play to an Apple TV on a separate network, configure the FortiWiFi unit according to these procedures:



- 1 Enable multicast forwarding and create security policies to allow multicast traffic. See [“Enable multicast forwarding”](#) on page 2.
- 2 Go to **Firewall Objects > Service > Custom** and select **Create New** to create a new custom service with these characteristics:

<b>Name</b>		AirPlay - OS X to Apple TV		
<b>Protocol Type</b>		TCP/UDP/SCTP		
<b>Protocol</b>	<b>Source Port Low</b>	<b>Source Port High</b>	<b>Destination Port Low</b>	<b>Destination Port High</b>
<b>TCP</b>	1	65535	7000	7000
<b>TCP</b>	1	65535	49152	49152
<b>UDP</b>	1	65535	1	65535

- 3 Select **OK**.

- 4 Select **Create New** to create another new custom service with these characteristics:

<b>Name</b>		AirPlay - Apple TV to OS X		
<b>Protocol Type</b>		TCP/UDP/SCTP		
<b>Protocol</b>	<b>Source Port Low</b>	<b>Source Port High</b>	<b>Destination Port Low</b>	<b>Destination Port High</b>
TCP	1	65535	3689	3689
UDP	1	65535	6002	6002

- 5 Select **OK**.
- 6 Go to **Policy > Policy > Policy** and select **Create New** to create a security policy to allow AirPlay traffic from the OS X computer network to the Apple TV network.

<b>Source Interface/Zone</b>	internal1
<b>Source Address</b>	all
<b>Destination Interface/Zone</b>	internal2
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	AirPlay - OS X to Apple TV
<b>Action</b>	ACCEPT

- 7 Select **OK**.
- 8 Select **Create New** to create a security policy to allow the AirPlay traffic from the Apple TV network to the OS X computer network.

<b>Source Interface/Zone</b>	internal
<b>Source Address</b>	all

<b>Destination Interface/Zone</b>	wlan
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	AirPlay - Apple TV to OS X
<b>Action</b>	ACCEPT

- 9 Select **OK**.
- 10 With this configuration in place, anyone using an iOS device on the wireless interface of the FortiWiFi unit can use AirPlay to play media on the Apple TV.