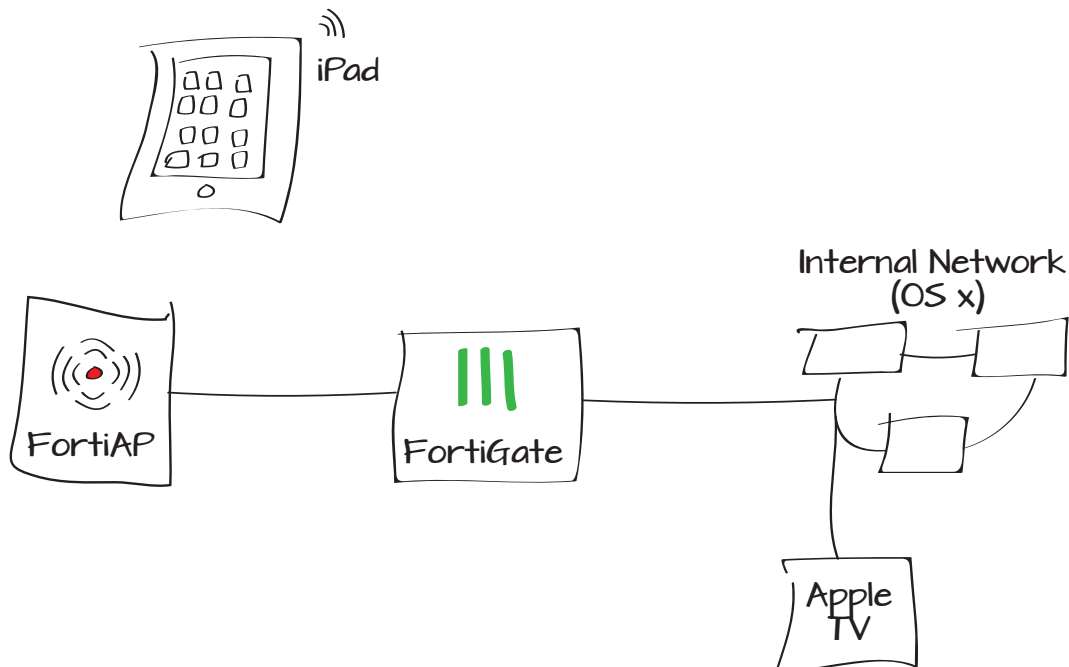


# Using AirPlay with iOS, AppleTV, FortiAP, and a FortiGate unit

This example sets up AirPlay services for use with an iOS device using Bonjour and multicast security policies.

1. Configuring the FortiAP and SSIDs
2. Adding addresses for the wireless network
3. Adding service objects for multicasting
4. Adding multicast security policies
5. Adding inter-subnet security policies
6. Results



# Configuring the FortiAP and SSIDs

Go to **System > Network > Interfaces**.

Edit the internal interface to be used for the FortiAP and set **Addressing Mode** to **Dedicate to FortiAP**.

Connect the FortiAP unit to the FortiGate unit.

Go to **WiFi Controller > Managed Access Points > Managed FortiAP** and authorize the FortiAP.

Once authorized, it will appear in the authorized list.

Name: dmz (00:09:0F:99:39:6B)  
Alias:   
Link Status: Up   
Type: Physical Interface

---

Addressing mode:  Manual  DHCP  PPPoE  Dedicate to FortiAP/F  
IP/Network Mask:   
1 Connected FortiAPs/FortiSwitches

---

Administrative Access:  HTTPS  PING  HTTP  FMG-Access  
 SSH  SNMP  TELNET  FCT-Access

IPv6 Administrative Access:  HTTPS  PING  HTTP  FMG-Access  
 SSH  SNMP  TELNET

---

Device Management  
Detect and Identify Devices:

Comments:  0/255

Administrative Status:  Up  Down

Mesh	Access Point	State	Connected Via	SSIDs
	FAP22B3U11022065		10.10.100.2	Radio 1: Radio 2:

- Edit
- Delete
- Authorize
- Restart
- Upgrade

Mesh	Access Point	State	Connected Via	SSIDs	Channels
	FAP22B3U11022065		10.10.100.2	Radio 1: All Radio 2: All	Radio 1: 3 Radio 2: 3

Go to **WiFi Controller > WiFi Network > SSID**.

Create a WiFi SSID for the network for wireless users and enable **DHCP Server**.

## Adding addresses for the wireless network

Go to **Firewall Objects > Address > Addresses**.

Create an address for SSID 1.

Name	WLAN1						
Type	WiFi SSID						
Traffic Mode	Tunnel to Wireless Controller						
IP/Network Mask	10.10.10.1/255.255.255.0						
IPv6 Address	:::0						
Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access						
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET						
DHCP Server	<input checked="" type="checkbox"/> Enable						
Address Range	<table border="1"><tr><td colspan="2">+ Create New Edit Delete</td></tr><tr><th>Starting IP</th><th>End IP</th></tr><tr><td>10.10.10.2</td><td>10.10.10.254</td></tr></table>	+ Create New Edit Delete		Starting IP	End IP	10.10.10.2	10.10.10.254
+ Create New Edit Delete							
Starting IP	End IP						
10.10.10.2	10.10.10.254						
Netmask	255.255.255.0						
Default Gateway	<input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify						
DNS Server	<input checked="" type="radio"/> Same as System DNS <input type="radio"/> Specify						
	<a href="#">Advanced...</a>						
WiFi Settings							
SSID	SSID1						
Security Mode	WPA/WPA2-Personal						
Data Encryption	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP-AES						
Pre-shared Key	..... (8 - 63 characters)						
Block Intra-SSID Traffic	<input type="checkbox"/>						
Maximum Clients	<input type="checkbox"/>						

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	SSID1_Subnet
Color	[Change]
Type	Subnet
Subnet / IP Range	10.10.10.0/255.255.255.0
Interface	WLAN1 (SSID: SSID1)
Show in Address List	<input checked="" type="checkbox"/>
Comments	Write a comment... 0/255

Create a second address for the internal network containing the OS X computers.

## Adding two service objects for AirPlay

Go to **Firewall Objects > Service > Services**.

Add service objects for each device connection.

Category  Address  IPv6 Address  Multicast Address

Name

Color

Type

Subnet / IP Range

Interface

Show in Address List

Comments  26/255

Name

Comments  0/255

Color

Show in Service List

Category

Protocol Type

IP/FQDN

Protocol	Destination Port		Source Port	
	Low	High	Low	High
TCP	7000	-		
UDP	1	- 65535		

Name

Comments  0/255

Color

Show in Service List

Category

Protocol Type

IP/FQDN

Protocol	Destination Port		Source Port	
	Low	High	Low	High
TCP	7000	-		
TCP	7100	-		
TCP	49152	- 50000		
UDP	1	- 65535		

## Adding multicast security policies

Go to **Policy > Policy > Multicast Policy**.

Create a policy to allow multicast traffic from the LAN and WLAN1 for AppleTV to iOS devices. Set **Incoming Interface** to LAN, **Source Address** to the Internal network, **Outgoing Interface** to the SSID, and **Destination Address** to Bonjour.



The Bonjour address allows the devices to find each other when they connect through the FortiGate unit.

Go to **Policy > Policy > Multicast Policy**.

Create a policy to allow multicast traffic from the WLAN1 and LAN for iOS devices to AppleTV. Set **Incoming Interface** to the SSID, **Source Address** to the SSID IP, **Outgoing Interface** to LAN, and **Destination Address** to Bonjour.

Incoming Interface	lan
Source Address	Internal network <span>+</span>
Outgoing Interface	WLAN1 (SSID: SSID1)
Destination Address	Bonjour <span>+</span>
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT <span>✓</span>
<input checked="" type="checkbox"/> Log Allowed Traffic	

Incoming Interface	WLAN1 (SSID: SSID1)
Source Address	SSID1_Subnet <span>+</span>
Outgoing Interface	lan
Destination Address	Bonjour <span>+</span>
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT <span>✓</span>
<input checked="" type="checkbox"/> Log Allowed Traffic	

## Adding inter-subnet security policies

Go to **Policy > Policy > Policy**.

Create a policy allowing traffic from the Apple TV to the iOS device. Set **Incoming Interface** to LAN, **Source Address** to the Internal network, and **Outgoing Interface** to the SSID.

Create a policy allowing traffic from the iOS device to the Apple TV. Set **Incoming Interface** to the SSID, **Source Address** to the SSID IP, and **Outgoing Interface** to the LAN.

## Results

Use AirPlay from the iPad to stream video to the Apple TV.

Go to **Log & Report > Traffic Log > Multicast Traffic** to see the multicast traffic between the WLAN1 and LAN interfaces.

Policy Type:  Firewall  VPN  
Policy Subtype:  Address  User Identity  Device Identity  
Incoming Interface: lan  
Source Address: Internal network  
Outgoing Interface: WLAN1 (SSID: SSID1)  
Destination Address: SSID1\_Subnet  
Schedule: always  
Service: AirPlay - Apple TV to iOS  
Action: ACCEPT  
 Enable NAT

Policy Type:  Firewall  VPN  
Policy Subtype:  Address  User Identity  Device Identity  
Incoming Interface: WLAN1 (SSID: SSID1)  
Source Address: SSID1\_Subnet  
Outgoing Interface: lan  
Destination Address: Internal network  
Schedule: always  
Service: AirPlay - iOS to apple TV  
Action: ACCEPT  
 Enable NAT

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Application Name	
4	09:49:41	WLAN1	lan	10.10.10.3	224.0.0.251	Unknown	3
5	09:47:28	lan	WLAN1	192.168.1.112	224.0.0.251	Unknown	2

Select an entry for more information.

<b>Dst</b>	224.0.0.251	<b>Virtual Domain</b>	root
<b>Received</b>	0	<b>Source Country</b>	Reserved
<b>Sent / Received</b>	300 B / 0 B	<b>Duration</b>	1237
<b>Sent</b>	300	<b>Application Details</b>	
<b>Service</b>	5353/udp	<b>Protocol</b>	17
<b>Destination Country</b>	Reserved	<b>Dst Port</b>	5353
<b>roll</b>	65498	<b>Status</b>	✓
<b>Timestamp</b>	Tue Apr 23 09:49:41 2013	<b>Tran Display</b>	noop
<b>Sequence Number</b>	0	<b>Policy ID</b>	5
<b>Src Interface</b>	WLAN1	<b>Src</b>	10.10.10.3
<b>Sent Packets</b>	3	<b>Level</b>	notice <span style="color:blue">■■■■■</span>
<b>Src Port</b>	5353	<b>Log ID</b>	12
<b>Sub Type</b>	multicast	<b>Threat</b>	
<b>Received Packets</b>	0	<b>Date/Time</b>	09:49:41 (Tue Apr 23 09:49:41 2013)
<b>Dst Interface</b>	lan		

<b>Dst</b>	224.0.0.251	<b>Virtual Domain</b>	root
<b>Received</b>	0	<b>Source Country</b>	Reserved
<b>Sent / Received</b>	232 B / 0 B	<b>Duration</b>	1105
<b>Sent</b>	232	<b>Application Details</b>	
<b>Service</b>	5353/udp	<b>Protocol</b>	17
<b>Destination Country</b>	Reserved	<b>Dst Port</b>	5353
<b>roll</b>	65498	<b>Status</b>	✓
<b>Timestamp</b>	Tue Apr 23 09:47:28 2013	<b>Tran Display</b>	noop
<b>Sequence Number</b>	0	<b>Policy ID</b>	6
<b>Src Interface</b>	lan	<b>Src</b>	192.168.1.112
<b>Sent Packets</b>	1	<b>Level</b>	notice <span style="color:blue">■■■■■</span>
<b>Src Port</b>	5353	<b>Log ID</b>	12
<b>Sub Type</b>	multicast	<b>Threat</b>	
<b>Received Packets</b>	0	<b>Date/Time</b>	09:47:28 (Tue Apr 23 09:47:28 2013)
<b>Dst Interface</b>	WLAN1		

Go to **Log & Report > Traffic Log > Log Forward** and filter policy IDs 6 and 7, which allow AirPlay traffic.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Pol
1	10:30:09	lan	WLAN1	192.168.1.110	10.10.10.3	7
2	10:28:24	lan	WLAN1	192.168.1.110	10.10.10.3	7
3	10:27:14	WLAN1	lan	10.10.10.3	192.168.1.110	6
4	10:26:34	WLAN1	lan	10.10.10.3	192.168.1.110	6
5	10:25:55	WLAN1	lan	10.10.10.3	192.168.1.110	6
6	10:25:25	WLAN1	lan	10.10.10.3	192.168.1.110	6
7	10:25:13	WLAN1	lan	10.10.10.3	192.168.1.110	6
8	10:24:46	WLAN1	lan	10.10.10.3	192.168.1.110	6
9	10:24:01	WLAN1	lan	10.10.10.3	192.168.1.110	6
10	10:24:01	WLAN1	lan	10.10.10.3	192.168.1.110	6

Select an entry for more information.



Apple TV can also be connected to the Internet wirelessly. AirPlay will function from any iOS device connected to the same SSID as Apple TV. No configuration is required on the FortiGate unit.

<b>Dst</b>	10.10.10.3	<b>Virtual Domain</b>	root
<b>Received</b>	2888	<b>Source Country</b>	Reserved
<b>Sent / Received</b>	2.82 KB / 2.82 KB	<b>Duration</b>	282
<b>Sent</b>	2888	<b>Application Details</b>	
<b>Service</b>	7010/udp	<b>Protocol</b>	17
<b>Destination Country</b>	Reserved	<b>Dst Port</b>	7010
<b>roll</b>	65498	<b>Status</b>	✓
<b>Timestamp</b>	Tue Apr 23 10:30:09 2013	<b>Tran Display</b>	noop
<b>Sequence Number</b>	10683	<b>Policy ID</b>	7
<b>Src Interface</b>	lan	<b>Src</b>	192.168.1.110
<b>Sent Packets</b>	38	<b>Level</b>	notice <span style="color: blue;">■■■■■■</span>
<b>Src Port</b>	7011	<b>Log ID</b>	13
<b>Sub Type</b>	forward	<b>Threat</b>	
<b>Received Packets</b>	38	<b>Date/Time</b>	10:30:09 (Tue Apr 23 10:30:09 2013)
<b>Dst Interface</b>	WLAN1		

<b>Dst</b>	192.168.1.110	<b>Virtual Domain</b>	root
<b>Received</b>	87986	<b>Source Country</b>	Reserved
<b>Sent / Received</b>	7.26 MB / 85.92 KB	<b>Duration</b>	28
<b>Sent</b>	7612538	<b>Application Details</b>	
<b>Service</b>	AirPlay	<b>Protocol</b>	6
<b>Destination Country</b>	Reserved	<b>Dst Port</b>	7100
<b>roll</b>	65498	<b>Status</b>	close
<b>Timestamp</b>	Tue Apr 23 10:27:14 2013	<b>Tran Display</b>	noop
<b>Sequence Number</b>	10994	<b>Policy ID</b>	6
<b>Src Interface</b>	WLAN1	<b>Src</b>	10.10.10.3
<b>Sent Packets</b>	5425	<b>Level</b>	notice <span style="color: blue;">■■■■■■</span>
<b>Src Port</b>	49625	<b>Log ID</b>	13
<b>Sub Type</b>	forward	<b>Threat</b>	
<b>Received Packets</b>	1667	<b>Date/Time</b>	10:27:14 (Tue Apr 23 10:27:14 2013)
<b>Dst Interface</b>	lan		