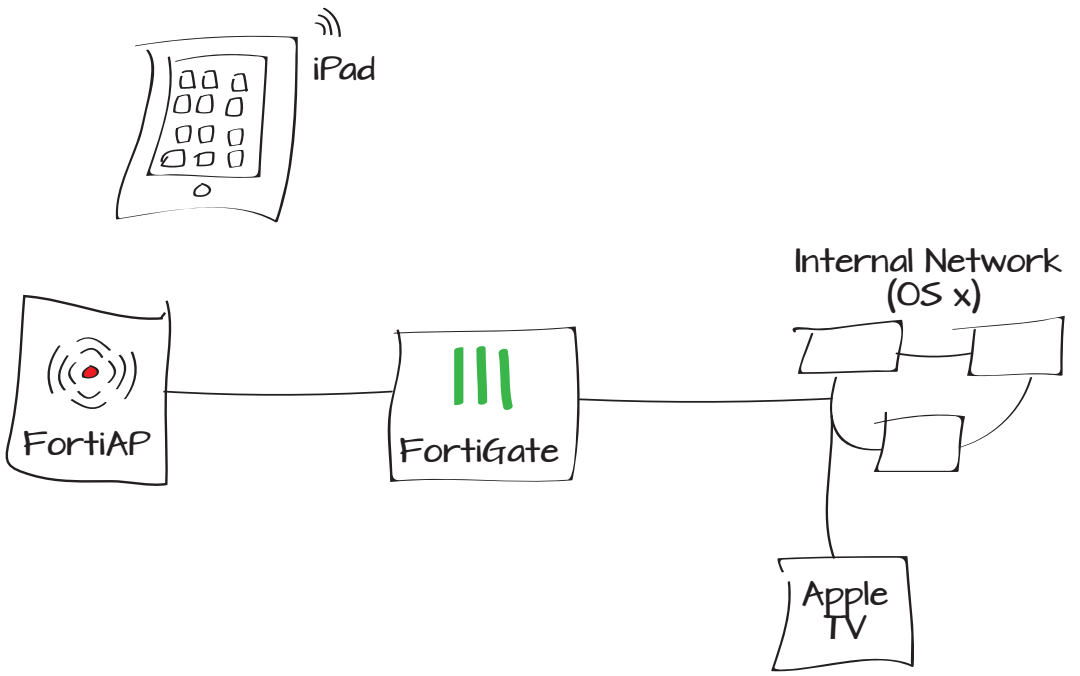
Using AirPlay with iOS, AppleTV, FortiAP, and a FortiGate unit

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

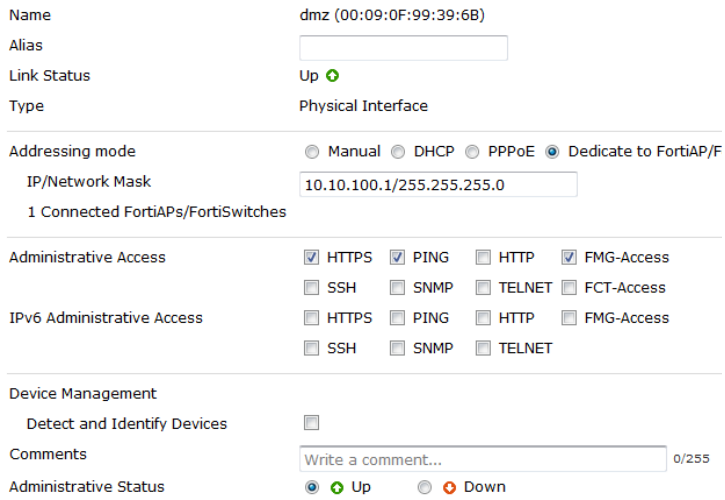
1. Configuring the FortiAP and SSIDs
2. Adding addresses for the wireless network
3. Adding service objects for multicasting
4. Adding multicast security policies
5. Adding inter-subnet security policies
6. Results



Configuring the FortiAP and SSIDs

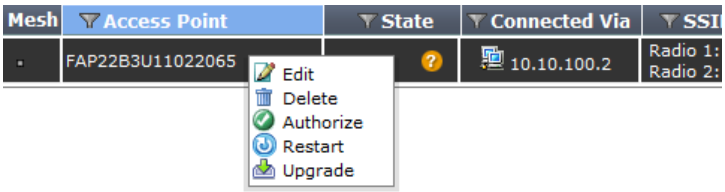
Go to **System > Network > Interfaces**.

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

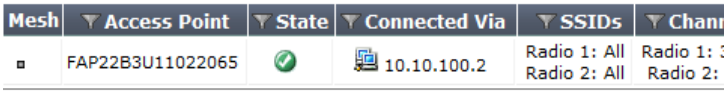


Connect the FortiAP unit to the FortiGate unit.

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

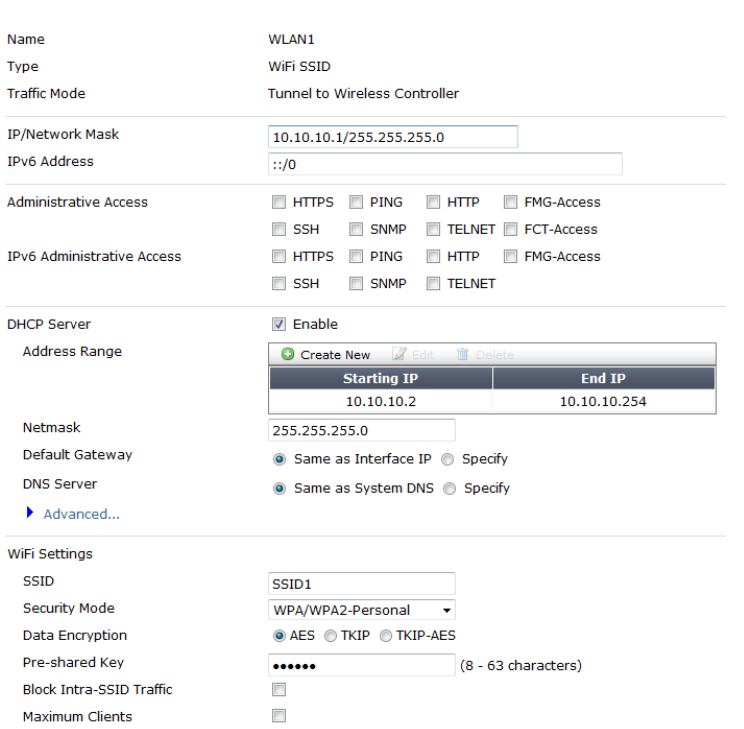


Once authorized, it will appear in the authorized list.



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

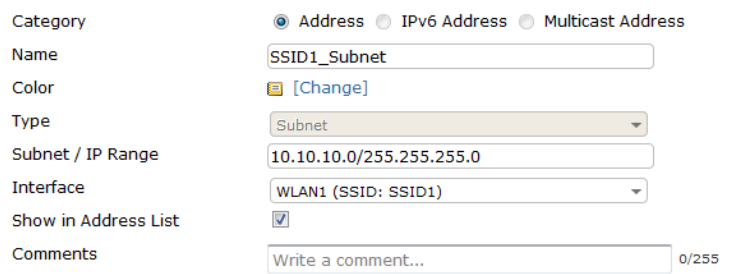
Create a WiFi SSID for the network for wireless users and enable **DHCP Server**.



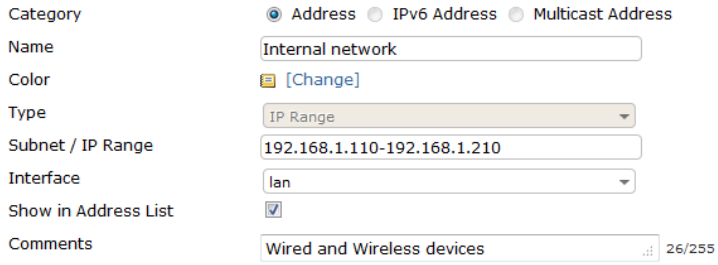
Adding addresses for the wireless network

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

Create an address for SSID 1.



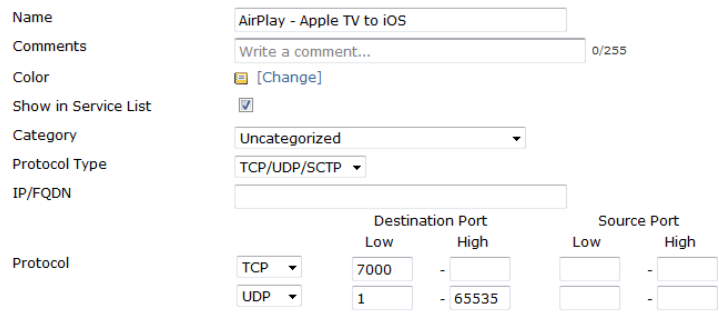
Create a second address for the internal network containing the OS X computers.

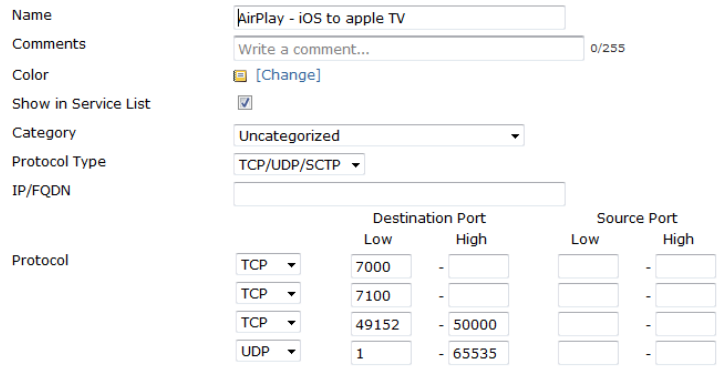


Adding two service objects for AirPlay

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

Add service objects for each device connection.



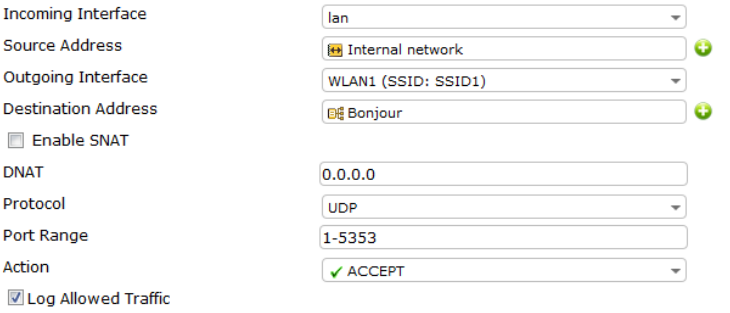


Adding multicast security policies

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

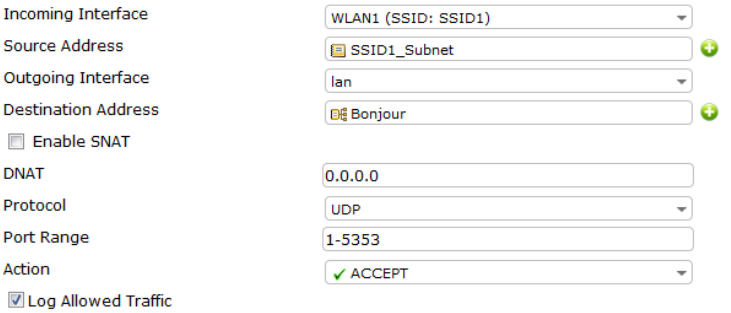
Create a policy to allow multicast traffic from the LAN and WLAN1 for AppleTV to iOS devices. Set **Incoming Interface** to LAN, **Source Address** to the Internal network, **Outgoing Interface** to the SSID, and **Destination Address** to **Bonjour**.

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



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

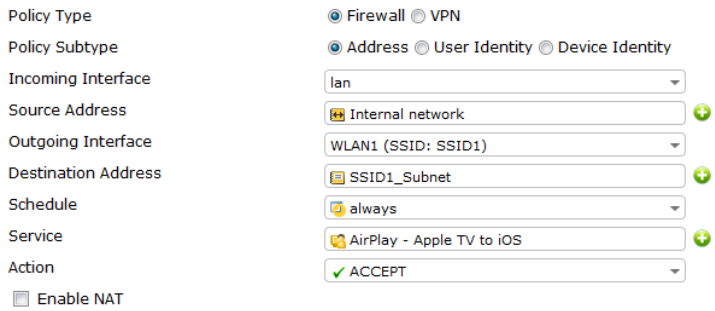
Create a policy to allow multicast traffic from the WLAN1 and LAN for iOS devices to AppleTV. Set **Incoming Interface** to the SSID, **Source Address** to the SSID IP, **Outgoing Interface** to LAN, and **Destination Address** to **Bonjour**.



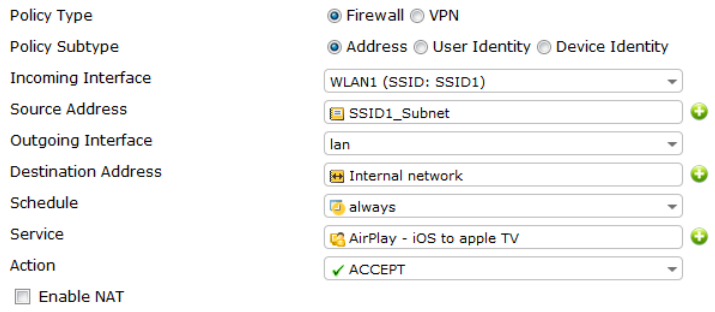
Adding inter-subnet security policies

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.



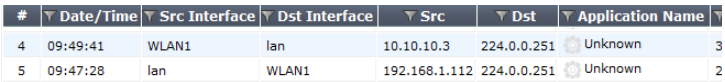
Create a policy allowing traffic from the iOS device to the Apple TV. Set **Incoming Interface** to the SSID, **Source Address** to the SSID IP, and **Outgoing Interface** to the LAN.



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.



#	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
5	09:47:28	lan	WLAN1	192.168.1.112	224.0.0.251	Unknown

Select an entry for more information.

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

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

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

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.

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