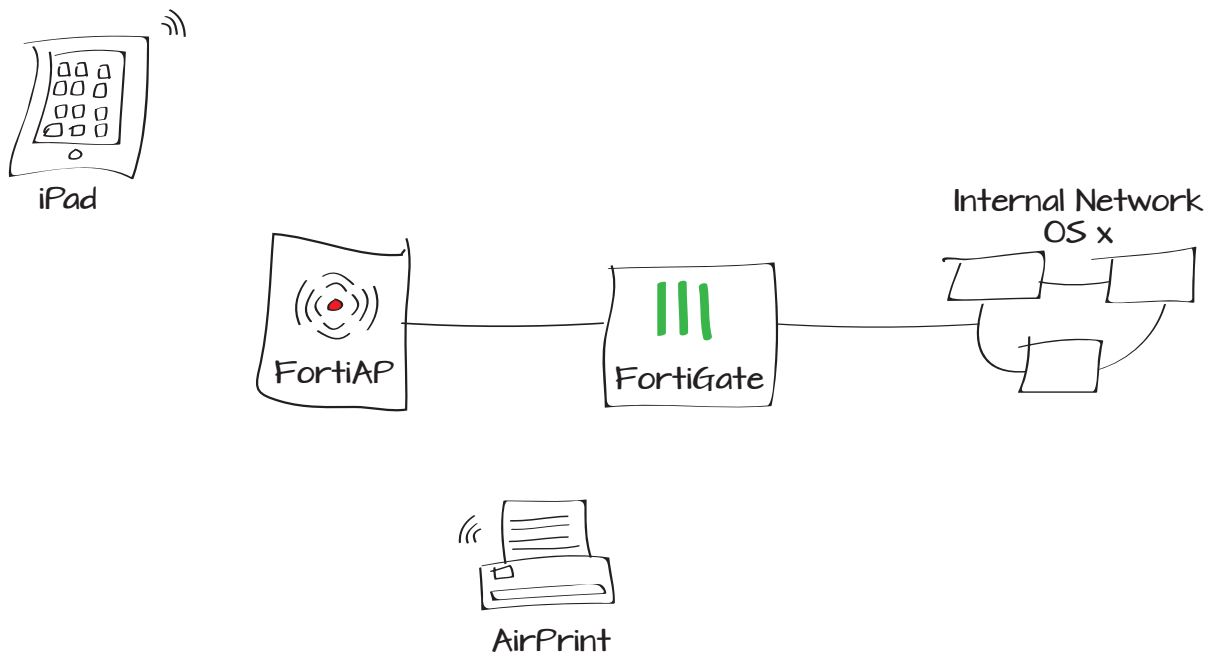


Using AirPrint with iOS and OS X and a FortiGate unit

This example sets up AirPrint services for use with an iOS device and OS X computers using Bonjour and multicast security policies.

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



Configuring the FortiAP and SSIDs

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

Set an internal interface as dedicated to the FortiAP unit.

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/FortiSwitch
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: All Radio 2: All

- Edit
- Delete
- Authorize
- Restart
- Upgrade

Mesh	Access Point	State	Connected Via	SSIDs	Chann
■	FAP22B3U11022065		10.10.100.2	Radio 1: All Radio 2: All	Radio 1: 3 Radio 2: (

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

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

Name	WLAN1				
Type	WiFi SSID				
Traffic Mode	Tunnel to Wireless Controller				
IP/Network Mask	<input type="text" value="10.10.10.1/255.255.255.0"/>				
IPv6 Address	<input type="text" value="::/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	<div style="border: 1px solid #ccc; padding: 2px;"><div style="display: flex; justify-content: space-between;">+ Create New Edit Delete</div><table border="1" style="width: 100%; border-collapse: collapse;"><thead><tr><th style="background-color: #333; color: white;">Starting IP</th><th style="background-color: #333; color: white;">End IP</th></tr></thead><tbody><tr><td style="text-align: center;">10.10.10.2</td><td style="text-align: center;">10.10.10.254</td></tr></tbody></table></div>	Starting IP	End IP	10.10.10.2	10.10.10.254
Starting IP	End IP				
10.10.10.2	10.10.10.254				
Netmask	<input type="text" value="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				
	▶ Advanced...				
WiFi Settings					
SSID	<input type="text" value="SSID1"/>				
Security Mode	<input type="text" value="WPA/WPA2-Personal"/> ▼				
Data Encryption	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP-AES				
Pre-shared Key	<input type="text" value="•••••"/> (8 - 63 characters)				

Create an SSID for the network for the AirPrint printer and enable **DHCP Server**.

Adding addresses for the wireless networks and printer

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

Create addresses for the SSID1, SSID2, and AirPrint printer.

Name	WLAN2						
Type	WiFi SSID						
Traffic Mode	Tunnel to Wireless Controller						
IP/Network Mask	20.20.20.1/255.255.255.0						
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>20.20.20.2</td><td>20.20.20.254</td></tr></table>	+ Create New Edit Delete		Starting IP	End IP	20.20.20.2	20.20.20.254
+ Create New Edit Delete							
Starting IP	End IP						
20.20.20.2	20.20.20.254						
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						
	Advanced...						
WiFi Settings							
SSID	SSID2						
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)						
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						
Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address						
Name	SSID2_Subnet						
Color	[Change]						
Type	Subnet						
Subnet / IP Range	20.20.20.0/255.255.255.0						
Interface	WLAN2 (SSID: SSID2)						
Show in Address List	<input checked="" type="checkbox"/>						
Comments	Write a comment... 0/255						

Create an address for the internal network containing the OS X computers.

Adding service objects for printing

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

Create a new service for Internet Printing Protocol (IPP) for iOS devices.

Create a new service for PDL Data Stream for OS X computers.

Category Address IPv6 Address Multicast Address

Name

Color

Type

Subnet / IP Range

Interface

Show in Address List

Comments 0/255

Category Address IPv6 Address Multicast Address

Name

Color

Type

Subnet / IP Range

Interface

Show in Address List

Comments 26/255

Name

Comments 26/255

Color

Show in Service List

Category

Protocol Type

IP/FQDN

Protocol	Destination Port		Source Port	
	Low	High	Low	High
TCP	631	-		

Name

Comments 15/255

Color

Show in Service List

Category

Protocol Type

IP/FQDN

Protocol	Destination Port		Source Port	
	Low	High	Low	High
TCP	9100	-		

Adding multicast security policies

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

Create two policies to allow multicast traffic from WLAN1 and WLAN2 for iOS devices.

For the first policy, set **Incoming Interface** to WLAN1, **Source Address** to the SSID1 IP, **Outgoing Interface** to WLAN2, and **Destination Address** to **Bonjour**.

For the second policy, set **Incoming Interface** to WLAN2, **Source Address** to the SSID2 IP, **Outgoing Interface** to WLAN1, and **Destination Address** to **Bonjour**.



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

Create two policies to allow multicast traffic from the LAN and WLAN2 for OS X computers.

For the first policy, set **Incoming Interface** to LAN, **Source Address** to the Internal network, **Outgoing Interface** to WLAN2, and **Destination Address** to **Bonjour**.

Incoming Interface	WLAN1 (SSID: SSID1)
Source Address	SSID1_Subnet
Outgoing Interface	WLAN2 (SSID: SSID2)
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

Incoming Interface	WLAN2 (SSID: SSID2)
Source Address	SSID2_Subnet
Outgoing Interface	WLAN1 (SSID: SSID1)
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

Incoming Interface	lan
Source Address	Internal network
Outgoing Interface	WLAN2 (SSID: SSID2)
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

For the second policy, set **Incoming Interface** to WLAN2, **Source Address** to the AirPrint, **Outgoing Interface** to LAN, and **Destination Address** to Bonjour.

Adding inter-subnet security policies

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

Create a policy allowing printing from wireless devices. Set **Incoming Interface** to WLAN1, **Source Address** to the SSID1 IP, **Outgoing Interface** to WLAN2, **Destination Address** to the AirPrint, and **Service** to IPP.

Create a policy allowing printing from an OS X computer to the AirPrint printer. Set **Incoming Interface** to LAN, **Source Address** to the Internal network, **Outgoing Interface** to WLAN2, **Destination Address** to the AirPrint, and **Service** to IPP.

Incoming Interface	WLAN2 (SSID: SSID2)
Source Address	AirPrint Printer IP
Outgoing Interface	lan
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	WLAN1 (SSID: SSID1)
Source Address	SSID1_Subnet
Outgoing Interface	WLAN2 (SSID: SSID2)
Destination Address	AirPrint Printer IP
Schedule	always
Service	IPP
Action	ACCEPT
<input type="checkbox"/> Enable NAT	

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	lan
Source Address	Internal network
Outgoing Interface	WLAN2 (SSID: SSID2)
Destination Address	AirPrint Printer IP
Schedule	always
Service	PDL
Action	ACCEPT
<input type="checkbox"/> Enable NAT	

Results

Print a document from an iOS device.


Go to **Log & Report > Traffic Log > Multicast Traffic** to see the printing traffic passing through the FortiGate unit.

Select an entry to see more information.

Go to **Log & Report > Traffic Log > Forward Traffic** and verify the entry with the IPP service.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Policy ID	Service
14	03-27 20:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
15	03-27 19:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
16	03-27 18:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
17	03-27 17:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
18	03-27 16:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
19	03-27 16:07	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
20	03-27 15:57	WLAN2	WLAN1	20.20.20.2	224.0.0.251	2	5353/udp
21	03-27 15:55	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
22	03-27 15:54	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
23	03-27 15:54	WLAN2	WLAN1	20.20.20.2	224.0.0.251	2	5353/udp

Dst	224.0.0.251	Virtual Domain	root
Received	0	Source Country	Reserved
Sent / Received	77 B / 0 B	Duration	17765
Sent	77	Application Details	
Service	5353/udp	Protocol	17
Destination Country	Reserved	Dst Port	5353
roll	65530	Status	✓
Timestamp	Wed Mar 27 20:44:11 2013	Tran Display	noop
Sequence Number	0	Policy ID	1
Src Interface	WLAN1	Src	10.10.10.3
Sent Packets	1	Level	notice ■■■■■
Src Port	5353	Log ID	12
Sub Type	multicast	Threat	
Received Packets	0	Date/Time	03-27 20:44 (Wed Mar 27 20:44:11 2013)
Dst Interface	WLAN2		

Dst	 20.20.20.2	Virtual Domain	root
Received	42012	Source Country	Reserved
Sent / Received	2.18 KB / 41.03 KB	Duration	2
Sent	2229	Application Details	
Service	631/tcp	Protocol	6
Destination Country	United States	Dst Port	631
roll	65530	Status	close
Timestamp	Wed Mar 27 15:35:41 2013	Tran Display	noop
Sequence Number	40762	Policy ID	3
Src Interface	WLAN1	Src	10.10.10.3
Sent Packets	27	Level	notice ■■■■■
Src Port	52549	Log ID	13
Sub Type	forward	Threat	
Received Packets	34	Date/Time	03-27 15:35 (Wed Mar 27 15:35:41 2013)
Dst Interface	WLAN2		

Print a document from an OS X computer.

Go to **Log & Report > Traffic Log > Multicast Traffic** to see the printing traffic passing through the FortiGate unit.

Select an entry to see more information.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Policy ID	Service
1	13:09:28	lan	WLAN2	192.168.1.112	224.0.0.251	4	5353/udp
2	12:09:28	lan	WLAN2	192.168.1.112	224.0.0.251	4	5353/udp
3	11:09:29	lan	WLAN2	192.168.1.112	224.0.0.251	4	5353/udp
4	10:32:57	lan	WLAN2	192.168.1.112	224.0.0.251	4	5353/udp
5	10:23:44	WLAN2	lan	20.20.20.2	224.0.0.251	2	5353/udp
6	10:23:44	WLAN2	lan	20.20.20.2	224.0.0.251	3	5353/udp

Dst	224.0.0.251	Virtual Domain	root
Received	0	Source Country	Reserved
Sent / Received	120 B / 0 B	Duration	417
Sent	120	Application Details	
Service	5353/udp	Protocol	17
Destination Country	Reserved	Dst Port	5353
roll	65526	Status	✓
Timestamp	Mon Apr 1 10:21:23 2013	Tran Display	noop
Sequence Number	0	Policy ID	4
Src Interface	lan	Src	192.168.1.112
Sent Packets	2	Level	notice
Src Port	5353	Log ID	12
Sub Type	multicast	Threat	

Refresh Download Raw Log

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Policy ID	Service
1	10:22:15	lan	WLAN2	192.168.1.112	20.20.20.2	5	9100
2	10:21:21	lan	WLAN2	192.168.1.112	20.20.20.2	5	9100
3	10:21:19	lan	WLAN2	192.168.1.112	20.20.20.2	5	9100
4	10:21:08	lan	WLAN2	192.168.1.112	20.20.20.2	5	9100

Go to **Log & Report > Traffic Log > Forward Traffic** and filter the destination interface for WLAN2 traffic.

Select an entry to see more information.

Dst	20.20.20.2	Virtual Domain	root
Received	532	Source Country	Reserved
Sent / Received	40.45 KB / 532 B	Duration	55
Sent	41416	Application Details	
Service	9100/tcp	Protocol	6
Destination Country	United States	Dst Port	9100
roll	65526	Status	close
Timestamp	Mon Apr 1 10:22:15 2013	Tran Display	noop
Sequence Number	3444	Policy ID	5
Src Interface	lan	Src	192.168.1.112
Sent Packets	33	Level	notice
Src Port	57631	Log ID	13
Sub Type	forward	Threat	
Received Packets	10	Date/Time	10:22:15 (Mon Apr 1 10:22:15 2013)
Dst Interface	WLAN2		